1. Barracuda Message Archiver - Overview . . . 4
1.1 What's New in Barracuda Message Archiver . . . 5
1.2 30 Day Evaluation Guide - Barracuda Message Archiver . . . 5
1.3 Deployment Options . . . 14
1.3.1 Microsoft Exchange Server Deployment . . . 14
1.3.1.1 How to Enable RPC over HTTP Connectivity . . . 15
1.3.1.2 How to Launch Barracuda Message Archiver from Microsoft Outlook Web Access . . . 20
1.3.1.3 Barracuda Message Archiver and Microsoft Exchange Server Migration . . . 21
1.3.1.4 SMTP or SMTP Relay Deployment Overview . . . 22
1.3.1.5 Microsoft Exchange Server 2013 Deployment . . . 23
1.3.1.5.1 Understanding Microsoft Exchange 2013 Journaling . . . 23
1.3.1.5.2 How to Configure Envelope (SMTP) Journaling for Microsoft Exchange Server 2013 - Standard Journaling . . . 24
1.3.1.5.3 How to Configure Envelope (SMTP) Journaling for Microsoft Exchange Server 2013 - Premium Journaling . . . 42
1.3.1.5.4 How to Configure an IMAP or POP3 Journal Account for Microsoft Exchange Server 2013 . . . 65
1.3.1.5.5 How to Disable Throttling in Microsoft Exchange Server 2013 . . . 69
1.3.1.6 Microsoft Exchange Server 2007 and 2010 Deployment . . . 70
1.3.1.6.1 Microsoft Exchange Server 2007 and 2010 Deployment Template . . . 70
1.3.1.6.2 Understanding Microsoft Exchange Server 2007 and 2010 Envelope Journaling . . . 74
1.3.1.6.3 Configuring Envelope Journaling for Microsoft Exchange Server 2007 and 2010 . . . 75
1.3.1.6.4 Configuring an IMAP or POP3 Journal Account for Microsoft Exchange Server 2007 and 2010 . . . 85
1.3.1.6.5 How to Disable Throttling in Microsoft Exchange Server 2007 and 2010 . . . 91
1.3.1.7 Microsoft Exchange Server 2003 Deployment . . . 91
1.3.1.7.1 Microsoft Exchange Server 2003 Deployment Template . . . 92
1.3.1.7.2 Understanding Microsoft Exchange 2003 Envelope Journaling . . . 95
1.3.1.7.3 Configuring an SMTP Journal Account for Microsoft Exchange 2003 . . . 96
1.3.1.7.4 Creating an Email Service Account for Microsoft Exchange Server 2003 . . . 127
1.3.1.7.5 Configuring an IMAP4 or POP3 Journal Account for Microsoft Exchange Server 2003 . . . 128
1.3.1.8 Creating an Email Service Account for Microsoft Exchange Server 2007, 2010, and 2013 . . . 132
1.3.2 High Availability Deployment . . . 134
1.3.2.1 Understanding Barracuda Message Archiver High Availability . . . 134
1.3.2.2 How to Prepare Systems for High Availability . . . 137
1.3.2.3 How to Join Systems in a High Availability Configuration . . . 138
1.3.2.4 How to Make Changes to an Existing High Availability Cluster . . . 140
1.3.2.5 How to Update Firmware and Energize Updates . . . 141
1.3.2.6 How to Remove or Replace a System . . . 141
1.3.3 CommuniGate Pro E-Mail Server Deployment . . . 142
1.3.4 Google Apps Deployment . . . 143
1.3.5 Barracuda Cloud Relay Service Configuration for Google Apps Mail Service . . . 147
1.3.6 GroupWise Deployment . . . 154
1.3.7 Kerio Connect Mail Server Deployment . . . 159
1.3.8 IBM Lotus Notes/Domino IMAP Deployment . . . 160
1.3.9 MailEnable Deployment . . . 167
1.3.10 MDaemon Messaging Server Deployment . . . 168
1.3.11 Barracuda Cloud Relay Service Configuration for Office 365 Mail Service . . . 169
1.3.12 Office 365 IMAP/POP Deployment . . . 172
1.3.13 Unix Mail Server Deployment . . . 175
1.3.14 Barracuda Message Archiver and the Barracuda Spam Firewall . . . 176
1.3.14.1 Understanding Email Encryption and Archival . . . 176
1.3.14.2 How to Set Up Email Encryption and Archival . . . 177
1.4 Getting Started . . . 179
1.4.1 Step 1: How to Install the Barracuda Message Archiver . . . 179
1.4.2 Step 2: How to Configure the Barracuda Message Archiver . . . 179
1.4.3 Step 3: How to Configure the Web Interface . . . 181
1.4.4 Step 4: How to Configure Administrative Settings . . . 183
1.4.4.1 Configuration Management and Access . . . 184
1.4.5 Step 5: Understanding Message Archiving Concepts . . . 187
1.5 Security . . . 189
1.5.1 Understanding Compliance . . . 190
1.5.2 How to Create Policy-Based Security . . . 191
1.5.3 How to Define Archived Message Retention Policies Based on Saved Searches . . . 193
1.5.4 How to Secure Network Access . . . 193

1.6 Backup and Storage . . . 194
1.6.1 Storage Backup . . . 194
1.6.1.1 Understanding Archived Data Backup . . . 196
1.6.1.2 How to Back Up Your Archived Data . . . 197
1.6.1.3 How to Back Up Your Barracuda Message Archiver . . . 198
1.6.1.4 Configuring a Data Partition Mirror . . . 200
1.6.1.5 Backing Up the Data Partition Using an External Solution . . . 201
1.6.2 Storage Manager . . . 202
1.6.2.1 Storage Details . . . 203
1.7 Accounts, Roles, and Email Aliases . . . 203
1.7.1 How to Manage User Accounts and Roles . . . 203
1.7.1.1 Auditor Role . . . 204
1.7.1.1.1 Viewing and Searching Messages - Auditor . . . 204
1.7.1.1.2 Saved Searches and Litigation Holds - Auditor . . . 206
1.7.1.1.3 Policy Alerts - Auditor . . . 206
1.7.1.1.4 Message Actions - Auditor . . . 207
1.7.2 Understanding Email Aliases . . . 208
1.7.3 Audit Log Filtering . . . 209
1.7.4 Adding LDAP Users . . . 210
1.7.4.1 LDAP User Include/Exclude Rules . . . 210
1.8 Message Import, Stubbing, and Configuration Options . . . 211
1.8.1 How to Import New Messages . . . 211
1.8.1.1 How to Set Up Email Journaling . . . 212
1.8.1.2 How to Archive Microsoft Non-Email Items . . . 213
1.8.1.3 How to Synchronize Folders . . . 213
1.8.1.4 How to Import GroupWise Messages . . . 213
1.8.1.4.1 Understanding GroupWise Trusted Application Keys . . . 214
1.8.1.4.2 How to Create a GroupWise Trusted Application Key . . . 214
1.8.1.5 How to Import IBM Notes NSF Files . . . 216
1.8.1.6 How to Configure Your Barracuda Message Archiver to Act as an SMTP Proxy to Your Email Server . . . 217
1.8.2 How to Import Historical Data . . . 218
1.8.3 Microsoft Exchange Server Integration . . . 220
1.8.4 Microsoft Exchange Server 2003, 2007, and 2010 Integration . . . 221
1.8.5 Understanding SMTP Forwarding and Trusted Servers . . . 226
1.8.6 Exchange Stubbing . . . 227
1.8.7 How to Retrieve Stubbed Messages in Shared Mailboxes . . . 229
1.8.8 Policy Alerts . . . 233
1.8.9 Retention Policies . . . 234
1.8.10 SMTP Proxy . . . 235
1.9 Search Options and Configuration . . . 236
1.9.1 Understanding Message Basics . . . 236
1.9.2 Viewing a Message . . . 236
1.9.3 Understanding Basic and Advanced Search . . . 237
1.9.3.1 Message Actions . . . 238
1.9.3.2 Advanced Search Tips . . . 239
1.9.3.3 Advanced Search Options . . . 240
1.9.3.4 Search Strings . . . 244
1.9.3.5 Keyword Expressions . . . 246
1.9.4 How to Set Up Saved Searches . . . 248
1.9.5 Global User Saved Search Filter . . . 249
1.9.6 Viewing Search-Related Activities . . . 250
1.9.7 Exchange Server 2010 SP1 Shared Mailbox Support . . . 251
1.9.7.1 Exchange Server 2010 SP1 Shared Mailbox Support Auto-Mapping . . . 252
1.9.8 How to Assign and Unassign PST Files . . . 253
1.10 Monitoring . . . 253
1.10.1 Viewing Performance Statistics . . . 254
1.10.2 Setting Up Alerts . . . 255
1.10.3 Viewing System Tasks . . . 256
1.10.4 Understanding the Front Panel Indicator Lights . . . 256
1.10.5 Reports . . . 257
1.10.5.1 Barracuda Message Archiver Usage Report . . . 258

1.11 Maintenance . . . 259
1.11.1 Configuration Backups . . . 259
1.11.2 Updating Your Firmware and Definitions . . . 260
1.11.3 Replacing a Failed System . . . 260
1.11.4 Reloading, Restarting, and Shutting Down the System . . . 261
1.11.5 Troubleshooting . . . 261
1.11.6 How to Reboot the System in Recovery Mode . . . 261
1.11.7 Migrating to a New Barracuda Message Archiver . . . 262
1.12 Tools and Add-Ins . . . 263
1.12.1 Barracuda Message Archiver Outlook Add-In . . . 263
1.12.1.1 Barracuda Message Archiver Outlook Add-In Deployment . . . 263
1.12.1.2 Installing and Configuring the Barracuda Message Archiver Outlook Add-In . . . 267
1.12.1.3 How to Search and Archive Messages Using the Barracuda Message Archiver Outlook Add-In . . . 273
1.12.1.4 Troubleshooting the Barracuda Message Archiver Outlook Add-In . . . 279
1.12.1.5 How to Enable the Barracuda Message Archiver Outlook Add-In in a Microsoft Terminal Server Environment . . . 281
1.12.1.6 Barracuda Outlook Add-In Customization Options . . . 283
1.12.1.7 How to Create Local Mailstores . . . 285
1.12.2 Barracuda Message Archiver Mobile Applications . . . 290
1.12.2.1 Barracuda Message Archiver Mobile Application for iPhone, iPod Touch, and iPad . . . 290
1.12.2.2 Barracuda Message Archiver Mobile Application for Android . . . 295
1.12.3 Barracuda PST Collector . . . 298
1.12.3.1 Option 1 - ADM with GPO Deployment . . . 300
1.12.3.2 Option 2 - ADM with Custom Deployment . . . 308
1.12.3.3 Option 3 - Command Line with Custom Deployment . . . 312
1.12.4 Barracuda Message Archiver Stand-Alone Search Utility . . . 317
1.12.4.1 Barracuda Message Archiver Stand Alone Search Utility - Windows Deployment . . . 317
1.12.4.2 Barracuda Message Archiver Stand-Alone Search Utility for Windows . . . 319
1.12.4.3 Barracuda Message Archiver Stand-Alone Search Utility for Mac OS X . . . 319
1.13 Hardware Compliance . . . 320
1.14 Limited Warranty and License . . . 320
1.15 Document Downloads . . . 330

Barracuda Message Archiver - Overview

The Barracuda Message Archiver is a complete and affordable email archiving solution designed for optimizing email storage, meeting regulatory compliance and e-discovery requirements, and providing anytime/anywhere access to old emails. The Barracuda Message Archiver integrates with all standards-based email servers and provides powerful search, retrieval, and export capabilities for administrators, auditors, and end-users.

Where to Start

- Step 1: How to Install the Barracuda Message Archiver
- Step 2: How to Configure the Barracuda Message Archiver
- Step 3: How to Configure the Web Interface
- Step 4: How to Configure Administrative Settings
- Step 5: Understanding Message Archiving Concepts

Alternatively, you can download the Barracuda Message Archiver Quick Start Guide including English, German, and Japanese translations.

Evaluation Guide

Use the 30-Day Evaluation Guide as a sample road map for setting up and testing the Barracuda Message Archiver in your organization's environment.

Key Features

- New Message Import – Depending on your network configuration, there are several ways in which the Barracuda Message Archiver can receive new messages (and other Microsoft Outlook items) for archiving.
- Import Historical Data – Archive any existing (stored) items that were either stored on your email server prior to setting up the Barracuda Message Archiver or stored in **.pst** files.
- Search Archived Content – Basic Search allows you to search archived content based on a word or phrase across all messages accessible by your account. Advanced Search allows you to run a complex search query based on multiple criteria; note that you can save queries for future use.
- Retention Policies – Set the maximum age of an archived message before it is permanently purged from the archive.
- Define Policies and Policy Alerts – In addition to built-in policy definitions, customize policies based on Saved Search criteria, and set up email notifications that are sent out when an incoming message that meets the policy criteria is detected.
- Exchange Stubbing – Enable stubbing to store attachments on the Barracuda Message Archiver rather than on the mail server itself to greatly increase the storage capacity of the mail server.
- Litigation Holds *(auditor role only)* – Define litigation holds to prevent messages that meet specific criteria from being removed from the Barracuda Message Archiver.
- Outlook Add-In – Synchronize archived folders with Microsoft Outlook, search for archived messages and other Outlook data, view and interact with your archived Outlook items, access stubbed attachments, and archive messages.
- Barracuda Message Archiver Companion Mobile Applications – Search for archived messages, search deleted messages, view and interact with your archived messages.

Deployment Options

The selected deployment mode is usually dependent on the email server configuration that currently exists at your site as well as the number of domains that are to be archived:

- Microsoft Exchange Server Deployment
- High Availability Deployment
- CommuniGate Pro E-Mail Server Deployment
- Google Apps Deployment
- Barracuda Cloud Relay Service Configuration for Google Apps Mail Service
- GroupWise Deployment
- Kerio Connect Mail Server Deployment
- IBM Lotus Notes/Domino IMAP Deployment
- MailEnable Deployment
- MDaemon Messaging Server Deployment
- Barracuda Cloud Relay Service Configuration for Office 365 Mail Service

- Office 365 IMAP/POP Deployment
- Unix Mail Server Deployment
- Barracuda Message Archiver and the Barracuda Spam Firewall

What's New in Barracuda Message Archiver

What's New in Release 3.5

- Shared Mailbox Support – Search shared mailboxes, and sync shared mailboxes to an offline store in Outlook
- New Mail Forwarding Options – Forward as an attachment, inline, or resend to your own mailbox
- Improved Microsoft Exchange Server Integration:
  - Exchange 2013 support
  - RPC over HTTPs
  - New Exchange Configuration page
  - Folder-based imports
- Archived Item Category – Specify whether to apply a category to items archived or stubbed by the Barracuda Outlook Add-In.
- Role and User Management
  - Assign Roles to LDAP Groups – When adding LDAP users and groups, associate a role with the account
  - Global User Saved Search Filter – Assign Filters to end-user searches
  - Create User Include/Exclude Rules – Create whitelist/blacklist rules when adding LDAP users and LDAP groups
- Export to Copy – Export messages to copy.com as either a zip or pst file.
- Export the Audit Log to a **.csv** file
- Set hourly Policy Alert notifications
- Dual-NIC and static routes on Barracuda Message Archiver model 650 and above
- Archived Data Recovery – Raw emails and metadata snapshot backup provides for rapid recovery in the event the data partition needs to be restored
- Barracuda Cloud Relay Service Configuration for Google Apps Mail Service
- Barracuda Cloud Relay Service Configuration for Office 365 Mail Service
- High Availability now synchronizes common configuration settings
- Updated iPhone and iPad, Android, and Macintosh OS X applications
  - Mobile Apps Support Email Address – Specify an email address to receive support queries from mobile application users

- Firmware version 3.5 requires version 1.5 or later of the Barracuda Message Archiver Mobile App for Android.
- Android phone or tablet running software version 2.3.3 or greater.
- Firmware version 3.5 requires version 3.5.0 (or later) of the Barracuda Message Archiver Mobile App for iOS, available for download from iTunes.
- The Barracuda Message Archiver Mobile App for iOS requires iOS 5.1 or later.
- Access for both Android and iOS mobile apps now requires an SSL connection to the Barracuda Message Archiver. If you are using one of the mobile apps from outside of your company network, your network administrator may need to update firewall/port-forwarding rules for secure access.

30 Day Evaluation Guide - Barracuda Message Archiver

This article refers to Barracuda Message Archiver firmware 3.5 and higher.

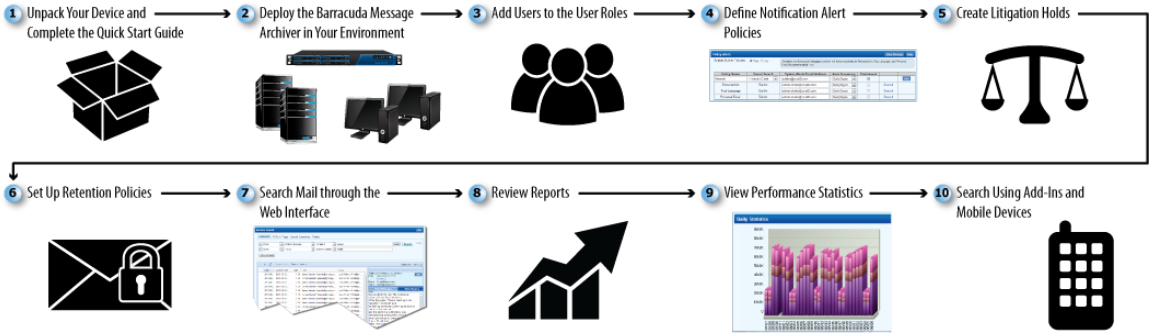
This article assumes you are logged in as the a*dministrator* (admin role) except where noted.

In this article:

- Step 1. Initial Setup and Configuration
- Step 2. Deployment Options
- Step 3. Add Users
  - Use Case – Add a User in the Auditor Role and Create a Custom Saved Search
- Step 4. Notification Alert Policies
  - Use Case – Custom Alert Policy
- Step 5. Litigation Holds – Auditor Role Only
  - Use Case – Litigation Hold

- Step 6. Retention Policies
  - Use Case – Global Retention Policy
- Step 7. Search Mail Using the Web Interface
  - Use Case – Export Messages
- Step 8. View Reports
  - Use Case – Automatically Generate Daily Reports
- Step 9. View Statistics
- Step 10. Tools and Add-Ins
  - Mobile Applications
    - Barracuda Message Archiver Mobile Application for Android
    - Barracuda Message Archiver Mobile Application for iPhone, iPod Touch, and iPad
  - Barracuda Message Archiver Outlook Add-In
  - Barracuda PST Collector
  - Barracuda Message Archiver Standalone Search Utility

Use this article as a sample road map for setting up and testing the Barracuda Message Archiver in your organization's environment:


1 Unpack Your Device and Complete the Quick Start Guide
2 Deploy the Barracuda Message Archiver in Your Environment
3 Add Users to the User Roles
4 Define Notification Alert Policies
5 Create Litigation Holds
6 Set Up Retention Policies
7 Search Mail through the Web Interface
8 Review Reports
9 View Performance Statistics
10 Search Using Add-Ins and Mobile Devices

Step 1. Initial Setup and Configuration

Go to the Getting Started section for complete installation and setup instructions, or use the Barracuda Message Archiver Quick Start Guide included with your Barracuda Message Archiver.

Step 2. Deployment Options

> **Hosted Email Service**
> If you do not have Email Servers and are using a hosted email service, please contact your Barracuda Networks Sales Engineer for deployment options.

Mail archival configuration is based on the Email Servers in your environment. Once you set up your Barracuda Message Archiver, determine the deployment that best suits your environment.

Once you complete your deployment configuration, mail begins forwarding to the Barracuda Message Archiver. Log in to the web interface as the administrator, and go to the **BASIC > Status** page. Processed mail displays in the **Message Statistics** table.

Step 3. Add Users

The Barracuda Message Archiver supports four user roles:

- **User** – The *user* can view and search content associated with their own mailbox and any shared mailboxes.
- **Auditor** – The *auditor* can view all items from any user, create and activate policies. Note that the auditor role can be restricted to specific domains by the Admin role.
- **IT Admin** – The *IT admin* can make system and network configuration changes only.
- **Admin** – The *admin* can view all items from any user, create and activate policies, and make system and network changes.

You set up users on the **USERS > User Add/Update** page. To retrieve a list of User Aliases from LDAP for the entered Email Address, click **Populate**.

Use Case – Add a User in the Auditor Role and Create a Custom Saved Search

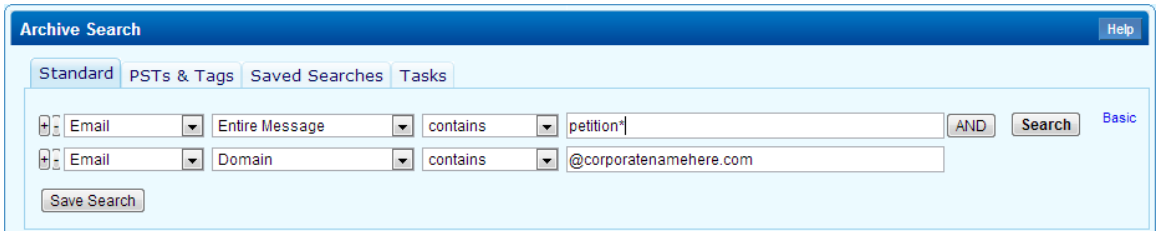
In this example, the administrator adds Jake in the auditor role. Jake has requested a custom Saved Search to automatically apply to all of his searches to reduce the number of items in the results pane. Jake wants only email related to petitions from the domain @corporatenamehere.com. Jake uses the following steps:

Click here to expand...

1. On the **BASIC > Search** page, click **Advanced**. Select **Email > Entire Message > contains**, type `petition*` as the first set of search criteria.

   > Using the '*' wildcard will return the words petition, petitions, petitioned, petitioner, and petitioning.

2. Click the + (plus) button to the left of the search parameter, select **Email > Domain > contains**, and type `@corporatenamehere.com` as the second set of search criteria:



3. Click **Search** to execute the search and verify that the provided search parameters return the expected results.
4. Click **Save Search**, enter `Petition Audit` as the name under which to save this search, and click **OK**.
5. Go to the **USERS > User Add/Update** page, enter **jake@corporateid.com**, and set **Use Email Address as Account Name** to **Yes**.
6. Click **Populate**; the system retrieves Jake's email aliases and displays them in the **User Aliases** field.
7. Enter Jake's password, and from the **Role** drop-down menu, select **Auditor**.
8. Leave the **Domains** field blank to allow Jake access to all items from all domains.
9. From the **Saved Search** drop-down menu, select **Petition Audit**, and then click **Save Changes** ; Jake is added as a user with the auditor role in the **Accounts** page.

Step 4. Notification Alert Policies

> **Additional Resources**
> For more information, refer to the article Policy Alerts, or log in to your Barracuda Message Archiver, go to the **POLICY > Alerts** page, and click **Help**.

You can enable policy alerts to send a notification to the administrator when corporate email is being used inappropriately or for non-business matters. Each time a message meeting the specified criteria is detected entering the Barracuda Message Archiver, an automatic email notification is sent based on the selected **Alert Frequency** on the **POLICY > Alerts** page.

To set up policy alerts, log in to the web interface, and on the **POLICY > Alerts** page, set **Enable Built-In Policies** to *Yes,* and click **Save Changes**. Built-In Policies include:

- **Personal Info** – Looks for Personally Identifiable Information inside messages. It scans for various formats of Social Security numbers, credit card numbers, and other types of potentially sensitive information.
- **Foul Language** – Looks for messages containing specific words that have been identified as *Foul Language*.
- **Personal Email** – Looks for messages sent to and from various sites that have been classified as non-business sites, such as recreation or gambling sites.

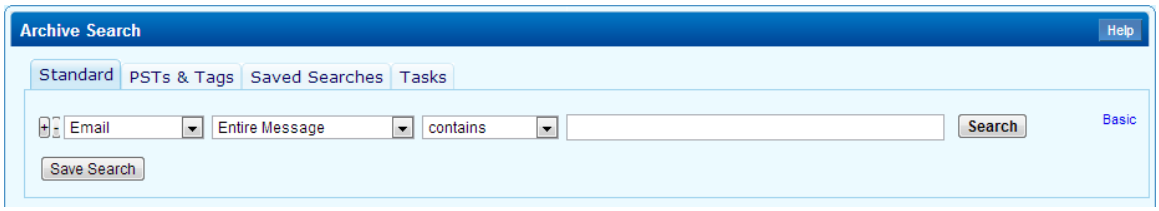
In addition to built-in policies, you can define custom policies based on a Saved Search that you create on the **BASIC > Search** page.

Use Case – Custom Alert Policy

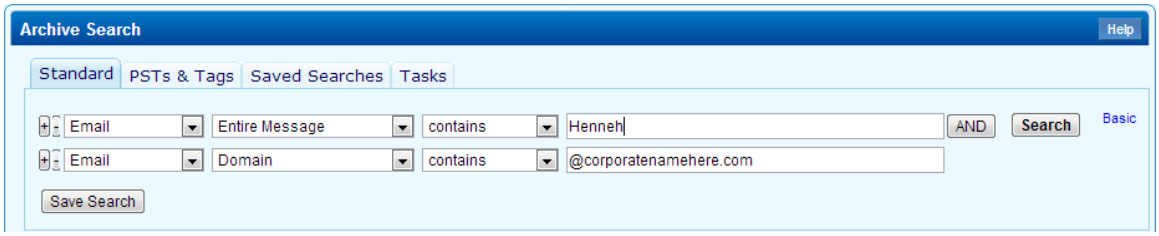
In this example, Joe is an administrator for the Barracuda Message Archiver at a local law firm. He has been asked to track any emails pertaining to their client 'Henneh' to or from the domain @corporatenamehere.com. Joe defines a custom alert policy in the Barracuda Message Archiver using the following steps:

Click here to expand...

1. On the **BASIC > Search** page, click **Advanced:**



2. Select **Email > Entire Message > contains**, type `Henneh` as the first set of search criteria, then click the **+** (plus) button to the left of the search parameter.
3. Select **Email > Domain > contains**, and type `@corporatenamehere.com` as the second set of search criteria:



4. Click **Search** to execute the search and verify that the provided search parameters return the expected results.
5. Click **Save Search**, enter `Henneh Client` as the name under which you wish to save this search, and click **OK**.
6. Now go to the **POLICY > Alerts** page, and enter `Henneh` as the **Policy Name**, select **Henneh Client** from the **Saved Search** drop-down menu, enter the alert email address `joe@mylawfirmname.com`, and set **Dashboard** to **On** so that the custom policy statistics display in the **Policy Statistics** table on the **BASIC > Status** page.
7. Click **Add** to save and activate the Policy Alert, and then click **Save Changes**.

Once activated, each time an email containing the client's name 'Henneh' that includes the domain '@corporatenamehere.com' in either the From, To, or Cc field, an alert notification is generated.

Important
Important:
If the Saved Search is deleted from the **Saved Search** tab on the **BASIC > Search** page, the custom alert policy is automatically deleted from the **POLICY > Alerts** page.

Step 5. Litigation Holds – Auditor Role Only

Additional Resources
For more information, refer to the article Litigation Holds, or log in to your Barracuda Message Archiver using the Auditor role, and go to either of the following pages:

- **POLICY > Retention** page, and click **Help**
- **BASIC > Search > Saved Search** page, and click **Help**

A user with the auditor role can create litigation holds to prevent messages that meet the criteria of a specific Saved Search from being removed from the Barracuda Message Archiver. On the **BASIC > Search > Saved Search** page, litigation hold details include:

- **Auditor** – The account name of the auditor who created the Litigation Hold
- **Saved Search** – The name of the Saved Search associated with this Litigation Hold
- **Hold End Date** – The date and time when this Litigation Hold expires

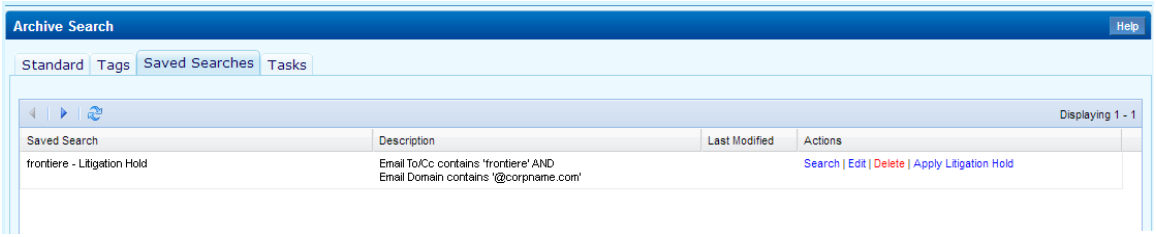
Before an auditor can set up a litigation hold, the administrator must first enable litigation holds by completing the following steps:

1. Log in to the Barracuda Message Archiver, and go to the **POLICY > Retention** page.
2. Set **Enable Litigation Holds** to **Yes**, and click **Save Changes.**

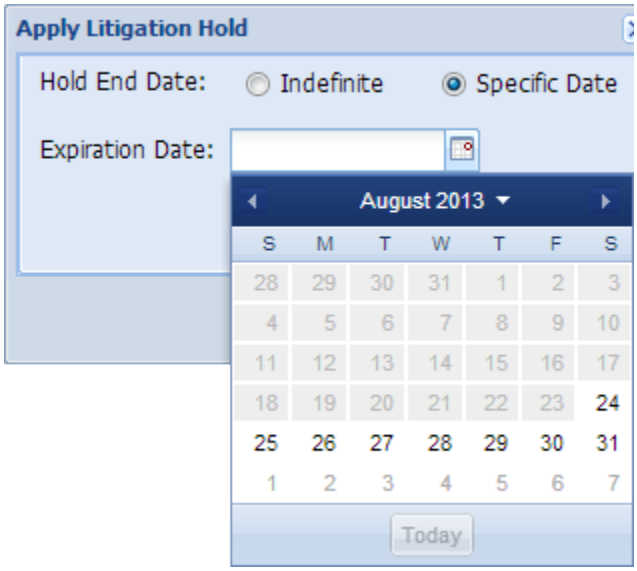
Use Case – Litigation Hold

In this example, Sue is an a user in the auditor role at a large corporation. She has been asked to set up a litigation hold:
Click here to expand...

1. Log in to the Barracuda Message Archiver in the auditor role.
2. Go to the **BASIC > Search** page, and click **Advanced**.
3. Select **Email > To/Cc > contains**, and type `fronteire` as the first set of search criteria. Click the **+** (plus) button to the left of the search parameter.
4. Select **Email > Domain > contains**, and type `@corpname.com` as the domain name.
5. Click **Search** to execute the search and verify that the provided search parameters return the expected results.
6. Click **Save Search**, enter `fronteire – Litigation Hold` as the name under which to save this search, and click **OK**.
7. Click the **Saved Searches** tab:



8. In the **Actions** column, click **Apply Litigation Hold**. In the **Apply Litigation Hold** window, you can specify to hold the associated emails as **Indefinite**, or click **Specific Date** to select an **Expiration Date**:


Apply Litigation Hold
Hold End Date:
Indefinite
Specific Date
Expiration Date:
August 2013
S M T W T F S
28 29 30 31 1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 31
1 2 3 4 5 6 7
Today

9. Click **OK** to apply the litigation hold.

Once a litigation hold is added, it displays in the **Litigation Holds** section on the **POLICY > Retention** page when a user is *logged in using the administrator role*:

Litigation Holds
Save Changes
Help
Enable Litigation Holds:
Yes
No
Allow auditors to create Litigation Holds. Items designated by a Litigation Hold are not subject to deletion by Retention Policies.
Litigation Holds created by system auditors. Messages matching these Saved Searches will be retained through the Hold End Date.
Auditor
Saved Search
Hold End Date
sueb
frontiere - Litigation Hold
2013-09-24 23:59:59

Step 6. Retention Policies

> **Additional Resources**
> For more information, refer to the article Retention Policies, or log in to your Barracuda Message Archiver, go to the **POLICY > Retention** page, and click **Help**.

By default, automatic message deletion is disabled on the Barracuda Message Archiver. However, your organization can select to expire messages based on the maximum age of messages. If automatic message deletion is enabled,

the Global Retention Policy and any Saved Search retention policies are run against all archived messages once a week. Note that before you can create a Saved Search retention policy, you must create at least one Saved Search in the **BASIC > Search > Advanced Search** page.

> **Important:**
> The Global Retention Policy setting does not apply to any messages that match a Saved-Search retention policy. If the age of any message exceeds the maximum age allowed by all Saved-Search retention policies that apply to the message, that message is *permanently deleted from the Barracuda Message Archiver*.

Use Case – Global Retention Policy

In this example, Kari is the administrator and wishes to set the maximum age of an archived message before it is permanently purged from the archive. Kari uses the following steps to set up retention using a Global Retention Policy:

Click here to expand...

1. Log in to the Barracuda Message Archiver as the administrator.
2. Go to the **POLICY > Retention** page, and set **Allow automatic message deletion** to **Yes**.
3. In the **Global Retention Policy** section, Kari determines the maximum number of days to retain messages. If she enters **0** in this field, the messages are kept indefinitely. She decides that messages should be retained for 30 days, and enters **30** in the **Policy Length** field.
4. Click **Save Changes**.

Once the Global Retention Policy is set, archived messages are automatically deleted from the Barracuda Message Archiver.

Step 7. Search Mail Using the Web Interface

> **Additional Resources**
> All user roles can view and search content associated with their own mailbox and any shared mailboxes.
>
> For more information, refer to the article Search Options and Configuration, or log in to your Barracuda Message, go to the **BASIC > Search** page, and click **Help**.

There are two search modes on the **BASIC > Search** page:

- **Basic** – Run a search based on a word or phrase across all messages accessible by your account.
- **Advanced** – Run a complex search query based on multiple criteria; note that you can save queries for future use.

When you initially go to the **BASIC > Search** page, all messages accessible by your account display in the message list in the **Standard** tab.

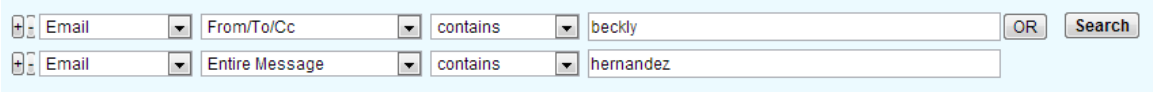
Use the Basic Search mode to perform a quick search across all of your messages. Use Advanced Search mode to perform complex search queries based on selected attributes.

Use Case – Export Messages

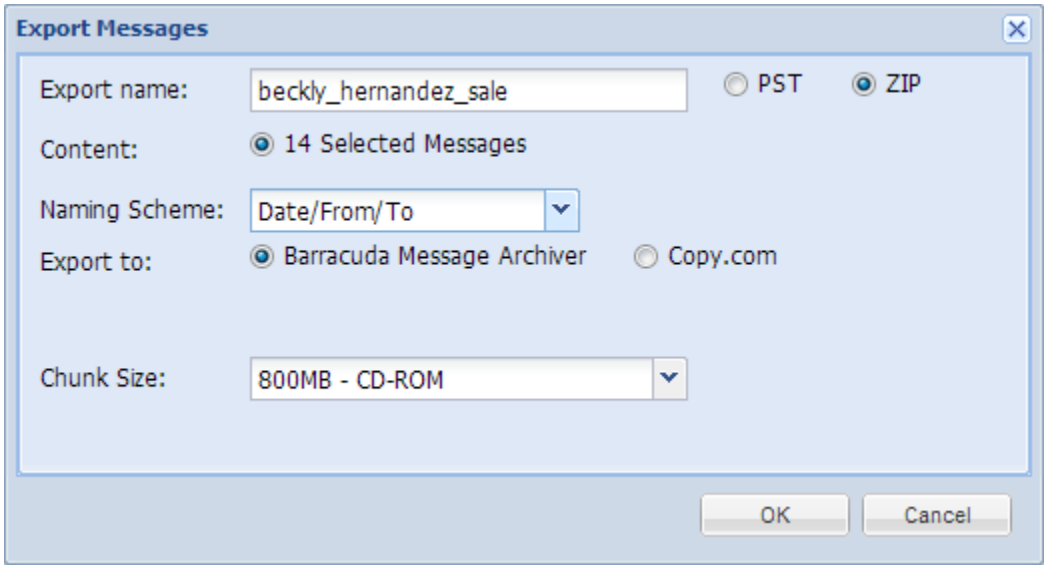
In this example, Uma works in a real estate office. She recently closed a sale for property on Hernandez Avenue with M. Beckly. The procedure in the office is to burn a CD with all correspondence regarding a sale once the sale is complete. Uma needs to search for all of messages related to the sale, and then export the messages to a .zip file:

Click here to expand...

1. Log in to the Barracuda Message Archiver as a user.
2. Go to the **BASIC > Search** page, and click **Advanced**.
3. Select **Email > From/To/Cc > contains**, and type **`beckly`** as the first set of search criteria, then click the **+** (plus) button to the left of the search parameter.
4. To the right of the first set of search criteria, click **AND** to toggle to **OR**.
5. Select **All > Entire Message > contains**, and type h**`ernandez`** as the second set of search criteria:



6. Click **Search** to execute the search and verify that the provided search parameters return the expected results.
7. In the results window, use **Ctrl-** and **Shift-**click to select all of the messages to include in the .zip file.
8. Click the **Tools** menu, and select **Export Messages**; in the **Export Messages** dialog box, specify the following details:
    a. Enter the **Export name** as `beckly_hernandez_sale`
    b. Select **ZIP**
    c. Select the **Naming Scheme** as **Date/From/To**
    d. Specify the **Export to** as **Barracuda Message Archiver** to download the ZIP file to your local system
    e. Specify the **Chunk Size** as **800 MB - CD-ROM**



9. Click **Save**.

UMA can now burn the ZIP file to a CD to place in M. Beckly's customer file.

Step 8. View Reports

> **Additional Resources**
> For more information, refer to the article Reports, or log in to your Barracuda Message Archiver, go to the **BASIC > Reports** page, and click **Help**.

The built-in reports on the Barracuda Message Archiver provide statistics on various operational, legal, and storage aspects. Default reports include message archive growth, policy violations, archive traffic, and cost analysis and projected archive storage growth.

On the **BASIC > Reports** page you can generate the following reports:

- **Email Activity Report** – View Barracuda Message Archiver email activity by user
- **Top Storage Users Report** – View Barracuda Message Archiver storage usage by user
- **Policy Violations Report** – View Barracuda Message Archiver email policy violations by user
- **Global Searches Report** – View the top Barracuda Message Archiver global searches by user
- **Usage Report** – Generate an overview of Barracuda Message Archiver cost analysis and projected archive storage growth

Use Case – Automatically Generate Daily Reports

In this example, the system administrator, Wiley, needs a daily report of policy violations by user. Wiley wants the reports sent to his administrator account wiley@corporateid.com, as well as to his boss, Francis, at francis@corporateid.com:

Click here to expand...

1. Log in to the Barracuda Message Archiver as a user.
2. Go to the **BASIC > Reports** page.
3. In the **Automated Reports** section, enter: `wiley@corporateid.com, francis@corporateid.com`
4. Click **Save Changes**.

Wiley and Francis will now receive a daily report of all policy violations, and the number of times each policy was violated, by user for the previous day. This report includes custom policies, and all built-in policies when enabled on the **POLICY > Alerts** page.

Step 9. View Statistics

> **Additional Resources**
> For more information, refer to the article Viewing Performance Statistics or log in to your Barracuda Message Archiver, go to the **BASIC > Status** page, and click **Help**.

View operating status on the **BASIC > Status** page when you log in to the Barracuda Message Archiver using either the auditor or administrator role as described in the following table:

Status Type	Description
Message Statistics	A snapshot of archived email, attachments, appointments, contacts, notes, and tasks.
Policy Statistics	Statistics for built-in and custom policies configured and selected on the **POLICY > Alerts** page.
Performance Statistics (1)	Current operating status and performance of the Barracuda Message Archiver including system load, fan speed, CPU temperature, storage percentages, redundancy.
Storage Statistics (1)	Statistics on the amount of data stored on the Barracuda Message Archiver by hour, day, and total.
Subscription Status (1)	Current status of your Energize Updates subscription, and the optional Instant Replacement and Premium Support subscriptions.
Cluster Status (1)	If you have joined two Barracuda Message Archivers in a High Availability configuration, the number of messages awaiting processing on the pair displays.
Hourly Statistics	Breakdown of message traffic and policy violations for the last 24 hours.
Daily Statistics	Breakdown of message traffic and policy violations for the last 30 days.
Notes: (1) Statistics for this item are not visible to auditors.	

Step 10. Tools and Add-Ins

> **Additional Resources**
> For more information, log in to your Barracuda Message Archiver, go to the **USERS > Client Downloads** page, and click **Help**.

You can download and install Barracuda Message Archiver tools and add-ins to your local system and mobile devices.

Mobile Applications

The Barracuda Message Archiver mobile application is available for Android and iPhone, iPod Touch, and iPad.

Barracuda Message Archiver Mobile Application for Android

The Barracuda Message Archiver mobile applications allow you to perform various actions with your messages that are stored on your organization's Barracuda Message Archiver, including:

- Search for archived messages based on email content, or constrain the search to a date range, a specific sender, or subject line content;

- Search deleted messages and emails no longer visible in your mail application;
- View and interact with (reply to, reply all, or forward) archived messages;
- Redeliver messages to your mailbox using the **Resend to Me** option.

These actions are available directly from your Android phone, allowing transparent access to, and interaction with, your archived messages.

> **Additional Resources**
> For configuration requirements, set up, and search options, refer to the Barracuda Message Archiver Mobile Application for Android article.

Barracuda Message Archiver Mobile Application for iPhone, iPod Touch, and iPad

The Barracuda Message Archiver mobile applications allow you to perform various actions with your messages that are stored on your organization's Barracuda Message Archiver, including:

- Search for archived messages based on email content, or constrain the search to a date range, a specific sender, or subject line content;
- Search deleted messages and emails no longer visible in your mail application;
- View and interact with (reply to, reply all, or forward) archived messages.

These actions are available directly from your iPhone, iPod Touch, or iPad, allowing transparent access to, and interaction with, your archived messages.

> **Additional Resources**
> For configuration requirements, set up, and search options, refer to the Barracuda Message Archiver Mobile Application for iPhone, iPod Touch, and iPad article.

Barracuda Message Archiver Outlook Add-In

The Barracuda Message Archiver Outlook Addin allows users to perform various functions with messages that are stored on your organization's Barracuda Message Archiver, including:

- Synchronization of your archived folders with Outlook
- Search for archived messages and other Microsoft Outlook data, such as Contacts
- View and interact with (forward, reply to, etc.) all of your archived Outlook items
- Access stubbed attachments
- Archive messages

These functions are available directly from within Outlook, allowing transparent access to your messages and attachments, all with no browser interaction required. All that is needed is a network connection to your organization's mail server and to the Barracuda Message Archiver.

> **Additional Resources**
> - For deployment options, refer to Barracuda Message Archiver Outlook Add-In Deployment.
> - For installation and configuration, refer to Installing and Configuring the Barracuda Message Archiver Outlook Add-In.
> - For details on searching and archiving messages, refer to How to Search and Archive Messages Using the Barracuda Message Archiver Outlook Add-In.

Barracuda PST Collector

Automated PST collection enables organizations to seamlessly meet litigation support and regulatory compliance requirements by simplifying the import of PSTs into the Barracuda Message Archiver. While the contents of individual PST files can be imported manually at any time, the Barracuda PST Collector automates the gathering and importing of pre-existing PST files from any directory on a Microsoft Windows-based system, minimizing the number of manual imports necessary to ensure that all emails are discoverable and included in the archive. The Barracuda PST Collector is available for Microsoft Windows-based systems only.

> **Additional Resources**
> For deployment options, refer to Barracuda PST Collector.

Barracuda Message Archiver Standalone Search Utility

The Stand-Alone Search Utility provides access to the search features of the Barracuda Message Archiver for Mac OS X and Microsoft Windows users. This utility allows users to search through their own archived messages directly from their desktop without needing to log in to the Barracuda Message Archiver web interface, and perform such actions as forwarding or replying to the located messages.

Additional Resources
For installation, configuration, and deployment details, refer to Barracuda Message Archiver Stand Alone Search Utility - Windows Deployment, or log in to your Barracuda Message Archiver, go to the **USERS > Client Downloads** page, and click **Help**.

Deployment Options

The selected deployment mode is usually dependent on the email server configuration that currently exists at your site as well as the number of domains that are to be archived.

In this Section

- Microsoft Exchange Server Deployment
- High Availability Deployment
- CommuniGate Pro E-Mail Server Deployment
- Google Apps Deployment
- Barracuda Cloud Relay Service Configuration for Google Apps Mail Service
- GroupWise Deployment
- Kerio Connect Mail Server Deployment
- IBM Lotus Notes/Domino IMAP Deployment
- MailEnable Deployment
- MDaemon Messaging Server Deployment
- Barracuda Cloud Relay Service Configuration for Office 365 Mail Service
- Office 365 IMAP/POP Deployment
- Unix Mail Server Deployment
- Barracuda Message Archiver and the Barracuda Spam Firewall

Related Articles

- Archiving Encrypted Email Messages (Barracuda Spam Firewall)

Microsoft Exchange Server Deployment

In this Section

- How to Enable RPC over HTTP Connectivity
- How to Launch Barracuda Message Archiver from Microsoft Outlook Web Access
- Barracuda Message Archiver and Microsoft Exchange Server Migration
- SMTP or SMTP Relay Deployment Overview
- Microsoft Exchange Server 2013 Deployment
- Microsoft Exchange Server 2007 and 2010 Deployment
- Microsoft Exchange Server 2003 Deployment
- Creating an Email Service Account for Microsoft Exchange Server 2007, 2010, and 2013

How to Enable RPC over HTTP Connectivity

This article refers to Barracuda Message Archiver firmware version 3.5 or higher, and Microsoft® Exchange™ Server.

RPC over HTTP (RoH), also known as Outlook Anywhere, is available for Exchange Integration in firmware 3.5 and higher, and is required by Exchange Server 2013. This connection may also be required with earlier versions of Exchange Server if the Barracuda Message Archiver cannot reach the Exchange Server directly, for example, if they are installed in different locations.

In this article:

- Enable RoH Capability
- Confirm RoH is Available
- Troubleshooting
  - Test Remote Connectivity
  - Test RoH Connectivity using Outlook

Related Articles

RoH must bind to your email service account; for details on setting up an email service account, refer to the following articles:

- Creating an Email Service Account for Exchange Server 2003
- Creating an Email Service Account for Exchange Server 2007, 2010, and 2013

Authentication
Basic authentication is required for the Barracuda Message Archiver to successfully connect to the RPC host; NTLM authentication is not available at this time.

SSL and SSL Certificates
SSL (HTTPS) must be enabled on the RoH proxy server. The RoH proxy server must be using a trusted, third-party certificate. If you have questions, or have the need to use privately signed certificates, contact Barracuda Networks Technical Support.

Note
If you are already using NTML authentication in your environment, you may want to set your RPC virtual directory to use both Basic and NTML authentication to avoid Outlook users being prompted for login information at each Outlook session. For additional information, see the Microsoft TechNet article RPC over HTTP Authentication and Security.

Enable RoH Capability

Use the following steps to enable RoH capability for Exchange integration:

1. Log in to the Barracuda Message Archiver web interface.
2. On the **MAIL SOURCES > Exchange Integration** page, click **Start New Action**.
3. Select an action, for example, **Email Stubbing**, and then click **Add New Server**.
4. Enter the Exchange Server details.

Exchange Server Details

Enter either your mailbox server hostname or your Exchange RPC Endpoint. For Exchange Server 2013, you can also use the

mailbox ID@domain format, for example:

d66ba-e2g8-48fb-9300-f64d01c52f2b@company.com

Important: This format is *required* for hosted Exchange 2013 providers.

For more information, refer to the Microsoft TechNet article What's New in Exchange 2013.

5. Once you have entered the Exchange Server details, click **Advanced Options**.
6. Enter the proxy server that is to provide RoH connectivity; that is, enter the Hostname of the RoH Proxy itself in the **Advanced > Proxy** field. RoH will be used if available.

Hosted Providers
If you are connecting to a hosted Exchange provider, the configuration provided by your vendor may not include all details necessary for the Barracuda Message Archiver. To determine the correct mailbox and RoH proxy servers, you can confirm your details using Microsoft's Exchange Connectivity Test site. For more information, refer to the Troubleshooting section below.

Exchange Configuration Testing

For information on testing your Exchange configuration using tools available from Microsoft, refer to the Troubleshooting section below. These tools will help confirm that details such as the required SSL certificates, Basic Authentication mode, and correct server name/ Exchange instance name and RoH proxy are being used.

Verify that both HTTP basic authentication and SSL (HTTPS) are enabled on the RoH proxy server; both are enabled by default. The RoH proxy server must be using a trusted, third-party certificate. If you have questions, contact Barracuda Networks Technical Support.

7. Click **Save**, and follow the onscreen directions to set up the action.

Note that if you have a scheduled action in the table you can also enable RoH using the following steps:

1. Click **Edit** in the **Scheduled Actions** table, and go to the **Select Server** page.
2. Click **Edit** following the server name, and click **Advanced Options** in the **Edit Server** page.
3. Enter the **Proxy Server**, Click **Save**, click **Continue** twice, and then click **Submit**.

Confirm RoH is Available

Use the following steps to confirm RoH is available to the Barracuda Message Archiver by testing through your browser:

1. Enter the Barracuda Message Archiver URI in a browser window in the form **https://*<proxy>*/rpc**, for example, `https://RoH server address/rpc`
2. Your browser should indicate that the RoH proxy's SSL certificate is trusted.
3. You should be challenged for your credentials by the browser; enter the Barracuda Message Archiver service account credentials.
4. Your credentials should be accepted, and you should see a blank page, be redirected to a different site, or receive an HTTP 503 error. This is expected. You should not encounter any *other* HTTP errors.

Troubleshooting

Use this section to test your Exchange configuration.

Test Remote Connectivity

Use Microsoft's Remote Connectivity Analyzer to test connectivity set up criteria, for example:

- Test whether Exchange Server is providing RoH
- Verify basic authentication is enabled; basic authentication is required
- Verify proper certificate chain is loaded

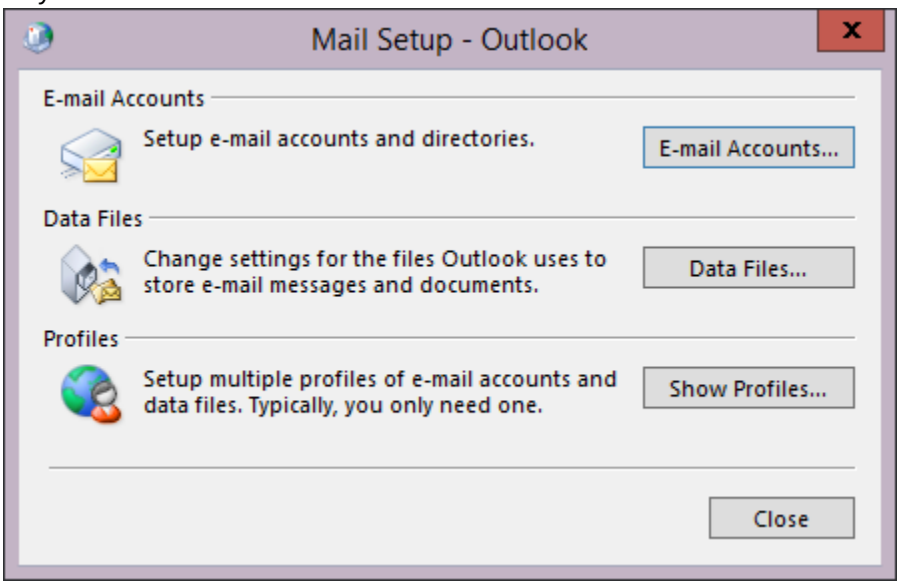
For example, from the **Exchange Server** tab you can test your Exchange Server RoH configuration, and from the **Client** tab you can download a standalone test client to your local workstation.

The remote connectivity tool is available from the Microsoft website: https://testconnectivity.microsoft.com/

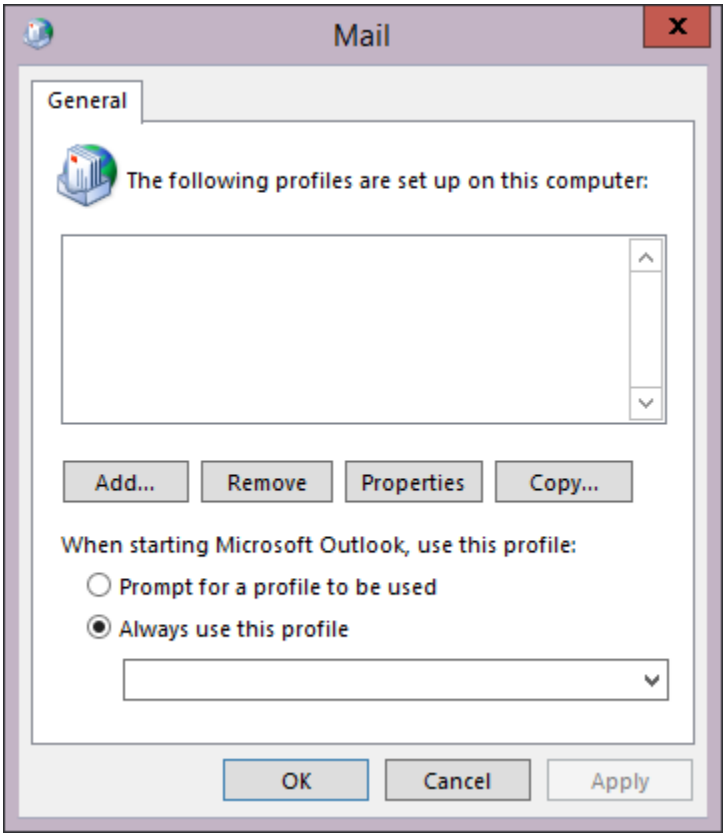
Test RoH Connectivity using Outlook

Use the following steps to verify your RoH configuration:

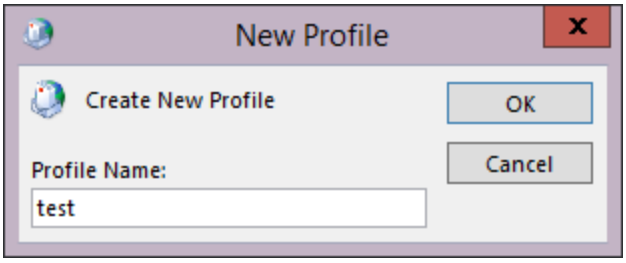
1. Go to the Mail applet in the Outlook **Control Panel**; the exact appearance of the Mail applet varies depending on your version of Windows and Outlook:


Mail Setup - Outlook
E-mail Accounts
Setup e-mail accounts and directories.
E-mail Accounts...
Data Files
Change settings for the files Outlook uses to store e-mail messages and documents.
Data Files...
Profiles
Setup multiple profiles of e-mail accounts and data files. Typically, you only need one.
Show Profiles...
Close

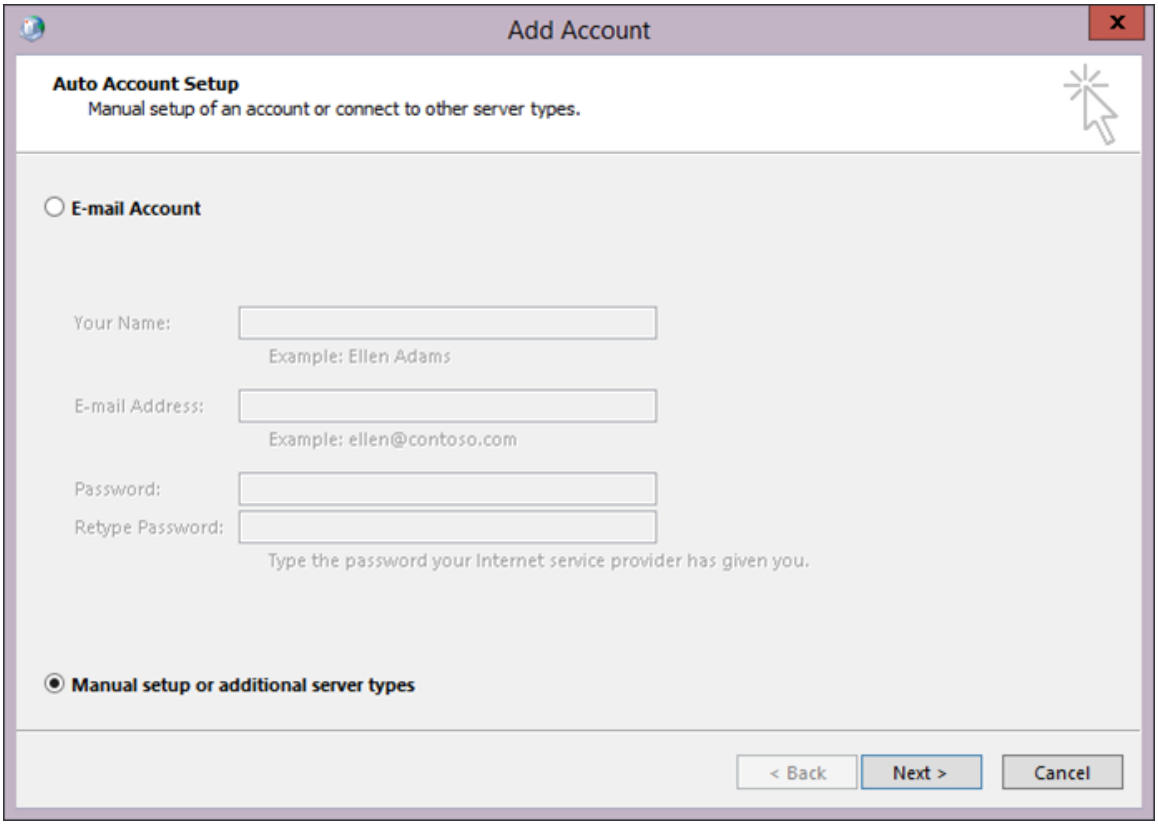
2. Click **Show Profiles**:



3. Click **Add** to create a temporary profile. Enter the **Profile Name**:

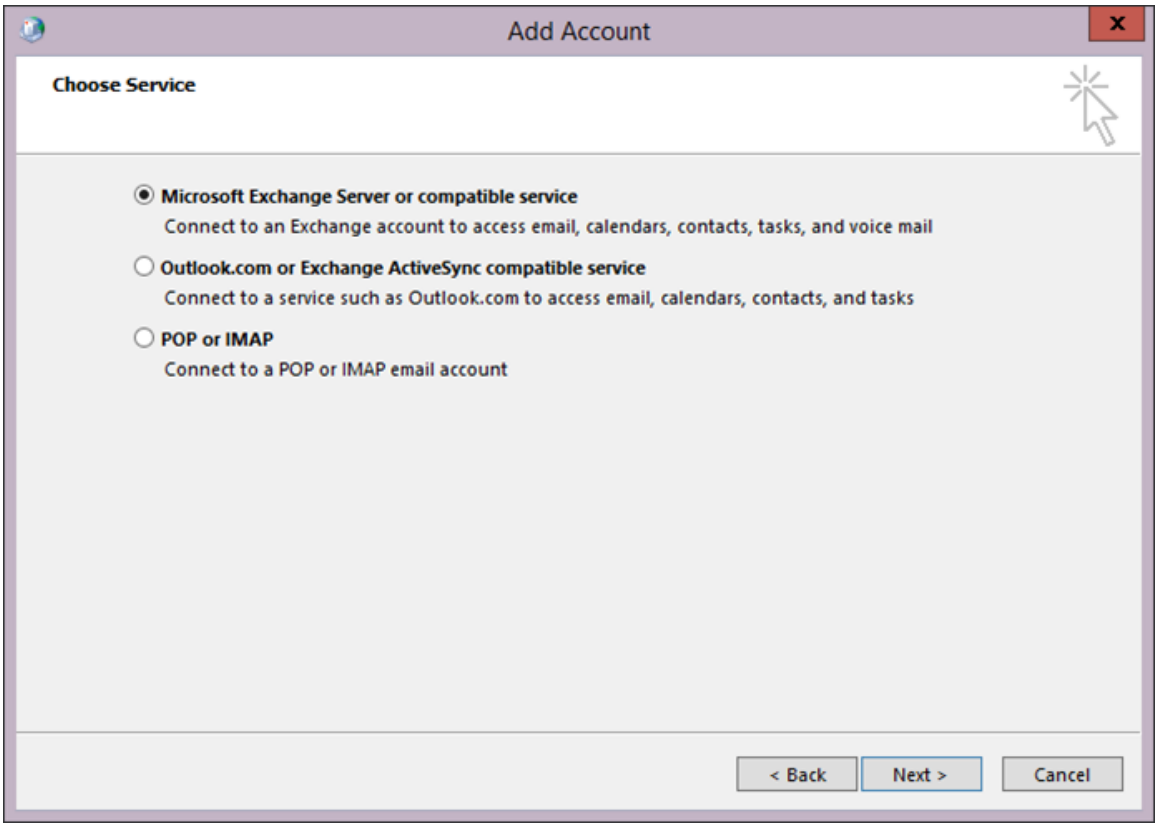


4. Click **OK**. In the **Add Account** page, select **Manual setup or additional server types**:

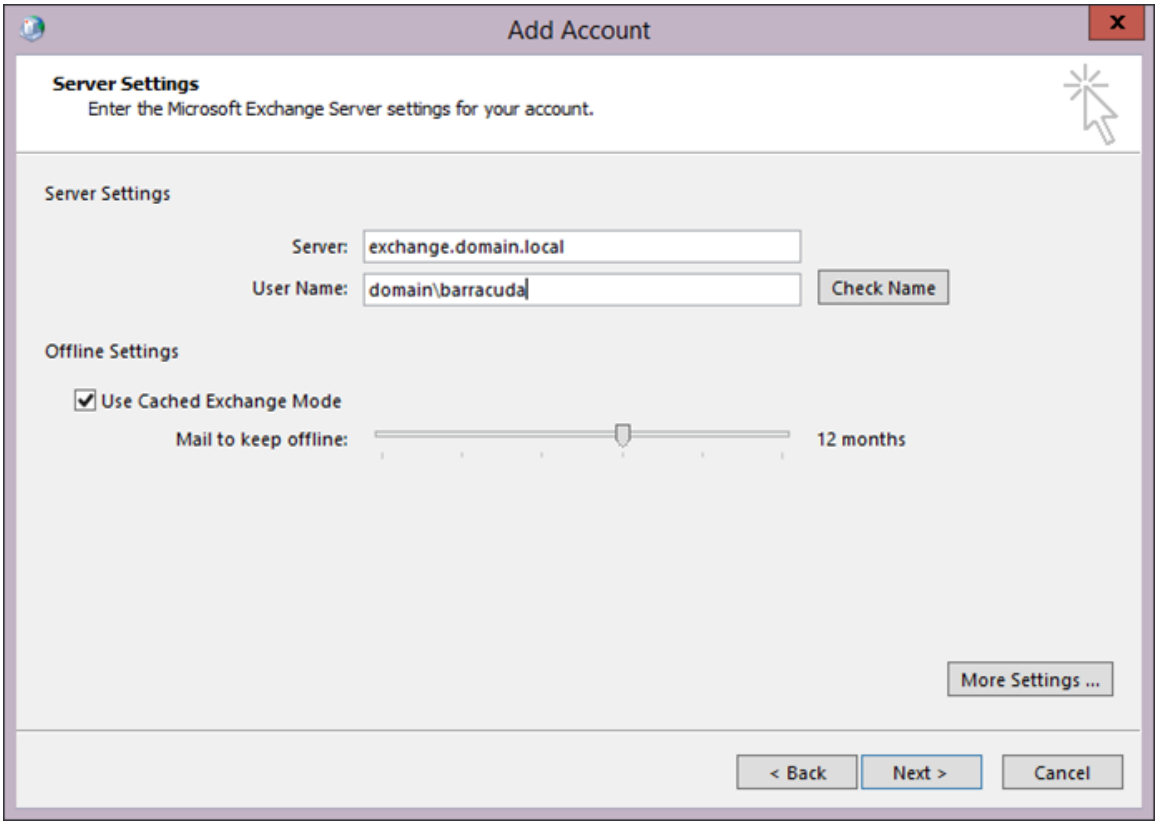


> Do not attempt to automatically configure this profile.

5. Click **Next**. Select **Microsoft Exchange Server or compatible service**:

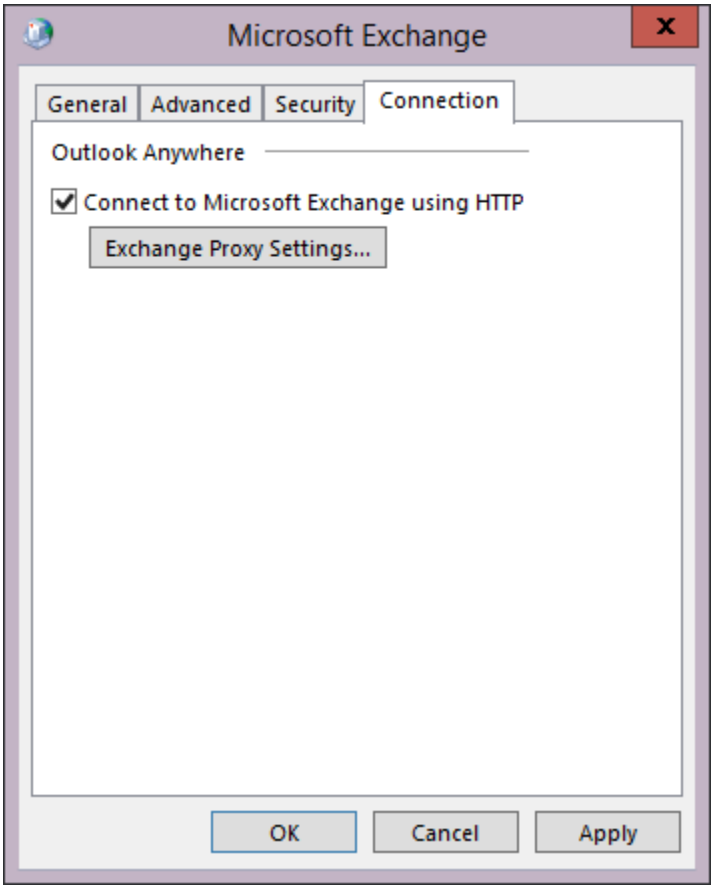

Add Account
Choose Service
Microsoft Exchange Server or compatible service
Connect to an Exchange account to access email, calendars, contacts, tasks, and voice mail
Outlook.com or Exchange ActiveSync compatible service
Connect to a service such as Outlook.com to access email, calendars, contacts, and tasks
POP or IMAP
Connect to a POP or IMAP email account
< Back
Next >
Cancel

6. Click **Next**. Enter the Exchange Server hostname in the **Server** field, and enter the Barracuda Message Archiver service account name in the **User Name** field:



7. Click **More Settings**. In the **Microsoft Exchange** dialog box, click the **Connection** tab, and turn on **Connect to Microsoft Exchange using HTTP**:

Depending on the version of Outlook you are running, warning messages may display alerting you to Exchange Server connection issues; this is expected as RoH is not yet configured. You can ignore these error messages at this step in the process.



8. Click **Exchange Proxy Settings**. In the **Microsoft Exchange Proxy Settings** dialog box, complete the following:
    - Enter the RoH proxy server hostname in the **https://** field.
    - Turn on **Connect using SSL only**.
    - Select **Basic Authentication** from the **Proxy authentication settings** drop-down menu.
9. Click **OK** to save your RoH configuration, and then click **OK** to close the **Microsoft Exchange** dialog box.
10. In the **Add Account** dialog box, click **Check Name**. You should be challenged for your credentials. Enter the Barracuda message Archiver service account credentials. You should be able to authenticate, and the username that you entered in the **Add Account** dialog should resolve successfully.
11. Click **Cancel** in the dialog box to remove the temporary Outlook profile. If a message displays asking if you want to create a profile without any email account, click **Cancel**.

How to Launch Barracuda Message Archiver from Microsoft Outlook Web Access

This article refers to the Barracuda Message Archiver release 3.2 or higher, Microsoft® Exchange Server 2007 or 2010, and Microsoft Outlook Web Access (OWA).

Additional Resources
• Outlook Web App User Customization for Exchange 2007 • Outlook Web App User Customization for Exchange 2010

Requirements
You must have the following privileges to complete these steps:

- Administrative privileges to your Microsoft Exchange Server
- Barracuda Message Archiver login credentials

Note that single sign-on (SSO) for OWA is not available at this time.

Use the following steps to add the Barracuda icon to the Microsoft OWA navigation bar:

1. Go to the Barracuda secure server, and download the Barracuda icon to your Exchange Server. The **.zip** file contains the following icons:
   - **LargeCuda.gif** (*large Barracuda icon, 24x24 pixels*)
   - **SmallCuda.gif** (*small Barracuda icon, 16x16 pixels*)
2. Unzip the files to the following directory based on your Exchange Server version:
   a. **Exchange 2010 – C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\Owa\forms\Customization**
   b. **Exchange 2007 – C:\Program Files\Microsoft\Exchange Server\ClientAccess\Owa\forms\Customization**
3. On your Exchange Server, browse to the **Customizations** folder where the icons are saved.
4. Locate and copy the file **UIExtensions.xml.template**, and rename the copied file **UIExtensions.xml**.
5. Open the **UIExtensions.xml** file in a text editor, and add the following content under the entry `<MainNavigationBarEntry`, replacing the URL *`https://example.company.com:443`* with your Barracuda Message Archiver URL including the protocol and port number:

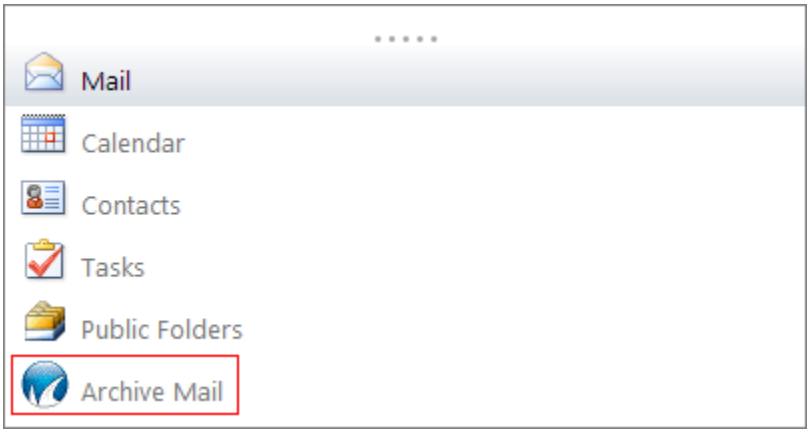
```
<MainNavigationBarExtensions>
    <MainNavigationBarEntry
            LargeIcon="LargeCuda.gif"
            SmallIcon="SmallCuda.gif"
            URL=" https://example.company.com:443 ">
        <string language="en-us" text="Archived Mail"/>
    </MainNavigationBarEntry>
</MainNavigationBarExtensions>
```

6. At a command line, run the following command to restart **Internet Information Service (IIS)**:

```
iisreset
```

> **IIS Restart**
> Users logged into OWA may be disconnected from their session when IIS is restarted.

7. Open Internet Explorer®, and log in to OWA.
8. At the end of your folder list, verify the Barracuda icon displays:



Barracuda Message Archiver and Microsoft Exchange Server Migration

This article refers to the Barracuda Message Archiver release 3.1 or higher, and Microsoft ® Exchange Server 2003, 2007, or 2010.

If you are deploying your Barracuda Message Archiver with a Microsoft Exchange Server and are planning to migrate to a newer version of Exchange Server, be aware of the following details based on the Barracuda Message Archiver features you have employed.

In this article:

- New Barracuda Message Archiver Deployment

- Existing Barracuda Message Archiver Deployment
- Relocating a Previously Deployed Barracuda Message Archiver

New Barracuda Message Archiver Deployment

If this is a new deployment, prior to migrating your Exchange Server, consider the following:

- You can deploy the Barracuda Message Archiver as a searchable “backup” of your email stores prior to migration to allow users to access all of their emails even when mail stores are unavailable during the Exchange migration.
- If you are upgrading to Exchange Server 2010 SP1 or higher, ensure that Microsoft’s “automapping” feature is enabled for the new Exchange Server integration with Active Directory (AD) for best performance by the Barracuda Message Archiver.
- You can set up the Barracuda Message Archiver to stub message attachments to reduce mailbox size prior to the Exchange Server migration, or to import all historic email content present on the Exchange Server prior to migration.

For complete deployment details, select appropriate deployment based on your Exchange Server environment.

Existing Barracuda Message Archiver Deployment

If you previously deployed the Barracuda Message Archiver with an Exchange Server and you are planning to migrate to a newer version of Exchange Server, consider the following:

- The Barracuda Message Archiver uses the unique user SID available for assigning PST files and folder information to AD users at the time of login. When you migrate to a newer version of Exchange Server, your users may receive a new SID. While users are still able to view all of their emails, they may not have PST or folder information available as that information on the Barracuda Message Archiver is associated with the original SID.
  To resolve this issue, at the time of migration, the Exchange Administer needs to populate the `sIDHistory` attribute on the new AD to establish a reference to the previous SID. In most instances this is all that is needed for the user to have full access to their historic folder and PST names. Contact Barracuda Networks Technical Support if you have additional questions or encounter any issues.
- Once the Exchange Server migration is complete, you may need to update the Barracuda Message Archiver’s Directory Services configuration, Exchange Integration configuration, and/or Journal Account information as appropriate for the new Exchange Server. For example, Exchange server local domain name, IP address, bind credentials, etc. must be updated.

Relocating a Previously Deployed Barracuda Message Archiver

If you previously deployed the Barracuda Message Archiver with an Exchange Server, and are planning to either relocate or change the local hostname of the Barracuda Message Archiver when migrating to a newer version of Exchange Server, the Barracuda Message Archiver, as well as any clients connecting to the Barracuda Message Archiver, may need to be updated with the new information including:

- Go to the **BASIC > Administration** page, and update the **External Access Configuration** section. The hostname in this page is used when linking stubbed attachments and *must* resolve to the Barracuda Message Archiver.
- If there are historic Stubbing URLs present on the Exchange Server that use an outdated hostname, Contact Barracuda Networks Technical Support for assistance with updating these stubbing links on the Exchange Server.
- Reconfigure the Outlook Add-In and end users with the new Barracuda Message Archiver location.
- Reconfigure the Barracuda Message Archiver Stand Alone Search Utility - Windows Deployment and end users with the new Barracuda Message Archiver location.

Contact Barracuda Networks Technical Support if you have additional questions or encounter any issues with migration.

SMTP or SMTP Relay Deployment Overview

Related Articles
• Message Import, Stubbing, and Configuration Options • Archiving Encrypted Messages (Barracuda Spam Firewall)

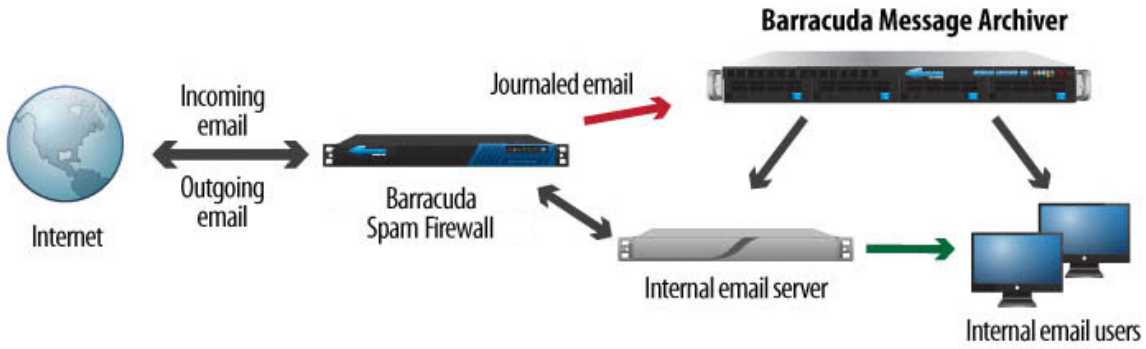
Additional Resource
• Barracuda Networks Knowledgebase Solution #00 002396

When journaling on your email server is not available or is not a practical option, you can use a combination of the Barracuda Message Archiver and the Barracuda Spam Firewall to capture both external and internal emails via SMTP. To capture messages sent from external Internet users, you can leverage the journaling capabilities of the Barracuda Spam Firewall to copy messages to your Barracuda Message Archiver. To capture

messages sent from inside your organization, you can configure internal email clients to use the Barracuda Message Archiver as an SMTP relay placed in front of your internal email server.

> If you are migrating to a newer version of Exchange Server, refer to the Barracuda Message Archiver and Microsoft Exchange Server Migration overview for more information.

The following image illustrates deployment through SMTP relay:



> The Barracuda Spam Firewall *only* forwards messages that it does *not* block to the Barracuda Message Archiver.

Microsoft Exchange Server 2013 Deployment

In this Section

- Understanding Microsoft Exchange 2013 Journaling
- How to Configure Envelope (SMTP) Journaling for Microsoft Exchange Server 2013 - Standard Journaling
- How to Configure Envelope (SMTP) Journaling for Microsoft Exchange Server 2013 - Premium Journaling
- How to Configure an IMAP or POP3 Journal Account for Microsoft Exchange Server 2013
- How to Disable Throttling in Microsoft Exchange Server 2013

> Full support for Exchange integration is available in Barracuda Message Archiver firmware version 3.5 or higher; support for Exchange Server 2013 Journaling is available in release 3.1 or higher. Mail sources/Exchange integration features for Exchange Server 2013 are available in firmware version 3.5 or higher.

Understanding Microsoft Exchange 2013 Journaling

This article refers to the Barracuda Message Archiver release 3.2 or higher, and Microsoft® Exchange Server 2013.

Microsoft Exchange 2013 provides the following journaling options:

- **Standard journaling** – Standard journaling is configured on a mailbox database. It enables the Journaling agent to journal all messages sent to and from mailboxes located on a specified mailbox database. To journal all messages to and from all recipients and senders, you must configure journaling on *all* mailbox databases on all mailbox servers in the organization.
- **Premium journaling** – Premium journaling enables the Journaling agent to perform more granular journaling by using journal rules. Instead of journaling all mailboxes residing on a mailbox database, you can configure journal rules to match your organization's needs by journaling individual recipients or members of distribution groups. You must have an Exchange Enterprise client access license (CAL) to use premium journaling.

When you enable standard journaling on a mailbox database, this information is saved in the Active Directory (AD) and is read by the Journaling agent. Similarly, journal rules configured with premium journaling are also saved in the AD and applied by the Journaling agent. For more information on configuring standard and premium journaling, refer to the Microsoft technet article Manage Journaling.

> Full support for Exchange integration is available in Barracuda Message Archiver firmware version 3.5 or higher; support for Exchange Server 2013 Journaling is available in release 3.1 or higher. Mail sources/Exchange integration features for Exchange Server 2013 are available in firmware version 3.5 or higher.

How to Configure Envelope (SMTP) Journaling for Microsoft Exchange Server 2013 - Standard Journaling

This article refers to the Barracuda Message Archiver firmware version 3.2 and higher, and a Microsoft® Exchange Server 2013 environment utilizing Standard Journaling, also known as mailbox database journaling.

If your Exchange environment has Premium Journaling capability, and you want more granular control over journaling, use the set up details in the article How to Configure Envelope (SMTP) Journaling for Microsoft Exchange Server 2013 - Premium Journaling.

Microsoft Exchange allows a Journal recipient to be either a *mailbox* or *contact*. By using a contact with an email address that is part of a non-existent domain, you can create a send connector that uses SMTP to deliver journaled mail to the Barracuda Message Archiver. Use the steps in this article to configure Envelope Journaling.

In this article:

- Step 1. Register Each Exchange Server as a Trusted SMTP Server
- Step 2. Create a Remote Domain From the Exchange Management PowerShell
- Step 3. Create a Recipient Mail Contact/Alternate Email Address
- Step 4. Create a Send Connector for the Remote Domain
- Step 5. Set Up Mailbox Database Journaling

Related Articles

- Understanding SMTP Forwarding and Trusted Servers

Full support for Exchange integration is available in Barracuda Message Archiver firmware version 3.5 or higher; support for Exchange Server 2013 Journaling is available in release 3.1 or higher. Mail sources/Exchange integration features for Exchange Server 2013 are available in firmware version 3.5 or higher.

Use the examples included in this article to simplify troubleshooting. Note that you can cut and paste the shell commands directly from this article.

Step 1. Register Each Exchange Server as a Trusted SMTP Server

To ensure that archiving begins as soon as your Exchange Servers are configured to send journal copies, first register each Exchange Server that is in a Client Access Server (CAS) role as a Trusted SMTP Server with the Barracuda Message Archiver on the **MAIL SOURCES** > **SMTP/IM** page in the web interface.

1a. Log into the Barracuda Message Archiver web interface, and go to the **MAIL SOURCES > SMTP/IM** page.

1b. In the **Trust SMTP Servers** section, enter the details for each Exchange Server that is to journal directly to the Barracuda Message Archiver; click **Add** after entering the details for each Exchange Server, and then click **Save Changes**.

Step 2. Create a Remote Domain From the Exchange Management PowerShell

The Remote Domain must *not* be your normal email domain. The remote domain must be a non-existent and non-routable/unresolvable domain from either inside or outside your organization (such as bma.int). This domain must be used for the email address of the Mail Contact that is to be the journaled message recipient.

> **Remote Domain**
> In previous versions of Exchange Server, the Exchange Management Console was used to create a Remote Domain; in Exchange Server 2013 the ECP/EAC has no analogous functionality so you must use PowerShell to create the Remote Domain.
>
> To create a Remote Domain, you must enter a **Name** to describe the domain, and the actual **Domain Name** to use. In this example, `bma.int` is the "fake" Domain Name that is used. You can use `bma.int` or create your own "fake" Domain Name. Note that this Domain Name is used when creating the **Mail Contact** in **Step 4**.

2a. Open Exchange Server 2013, and click **Exchange Management Shell**.

2b. Execute the following command to create the remote domain; this command ensures TNEF encloding is disabled and auto-forwarding is enabled:

```
New-RemoteDomain -DomainName bma.int -Name "Message Archiver Domain"

Get-RemoteDomain | Where {$_.DomainName -eq "bma.int"} | Set-RemoteDomain -TNEFEnabled $false
-AutoForwardEnabled $true
```

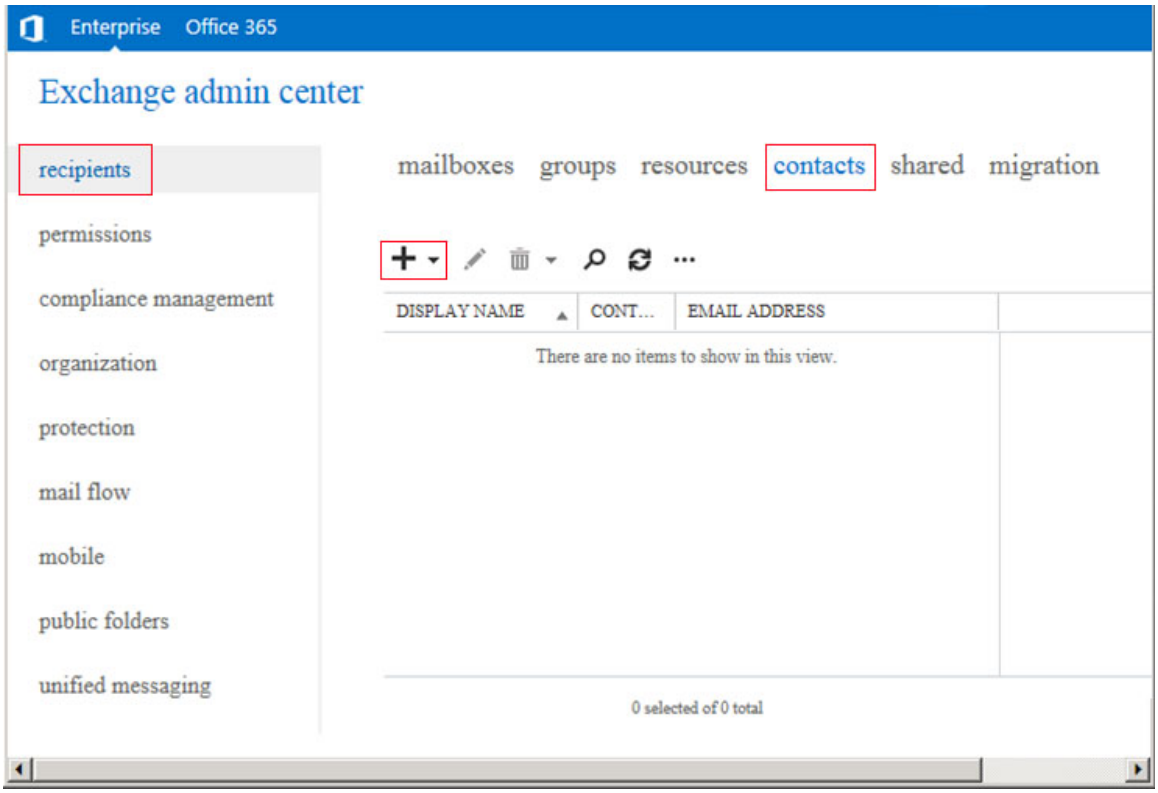
2c. Enter the following command to verify the settings:

```
Get-RemoteDomain | Where {$_.DomainName -eq "bma.int"} |Format-table Name, DomainName, TNEFEnabled,
AutoForwardEnabled
```

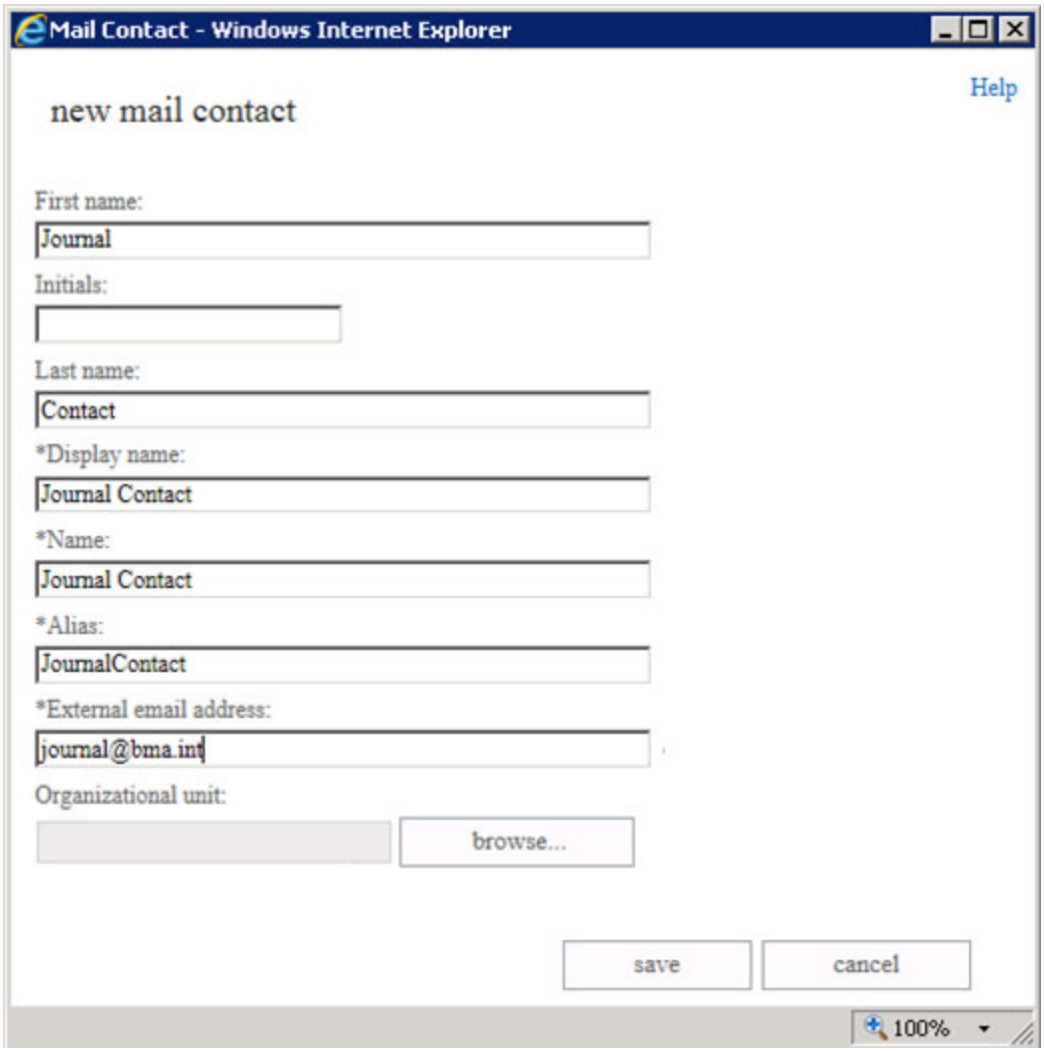
Step 3. Create a Recipient Mail Contact/Alternate Email Address

The Mail Contact is the account that is to act as a "holding location" for journaled messages. The email address associated with this account is the designated recipient and must be associated with a non-existent, non-routable dummy Domain Name created above in **Step 2**. Use the following steps to create the Mail Contact:

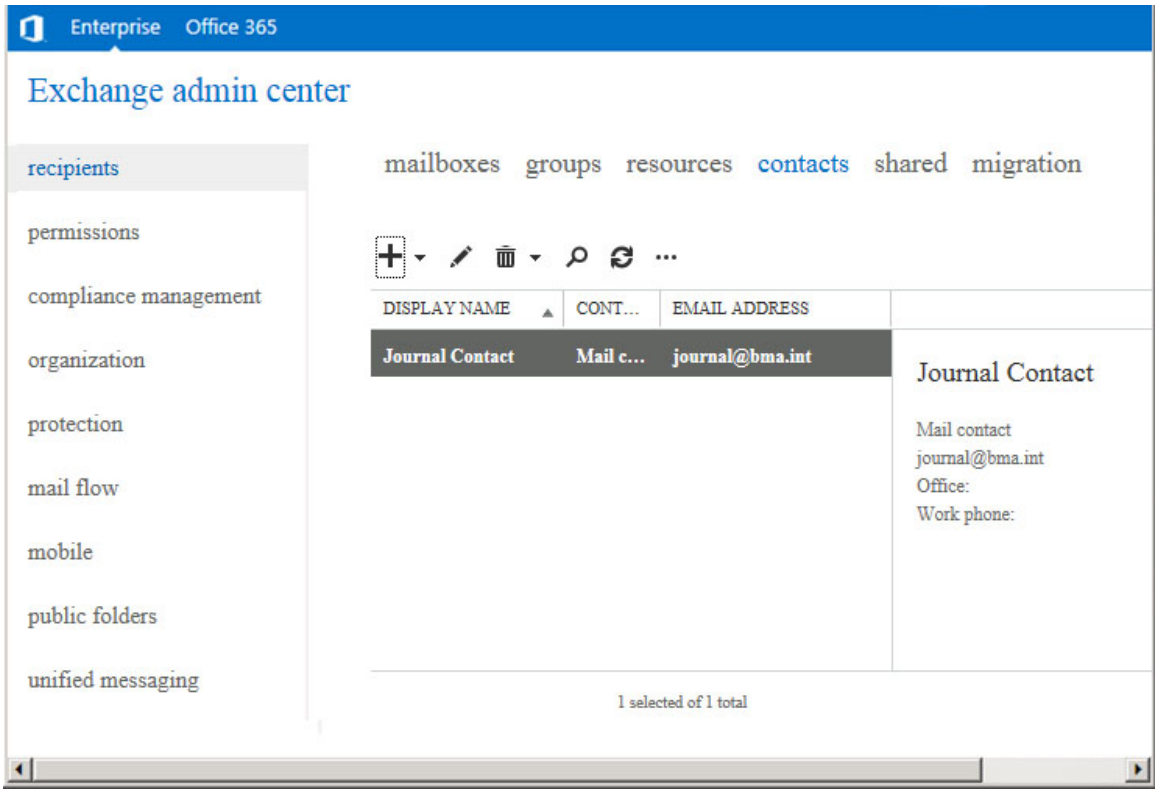
3a. Open Exchange Server 2013, and in the Exchange Admin Center (EAC) click **recipients** in the left pane, select **contacts** at the top of the page, and then click the **Add** (+) icon to create a new mail contact:



3b. In the **new mail contact** page, enter details for the designated recipient account details:



3c. Click **save**. The new contact displays in the **contacts** list:



Hide Contact from Global Address List
Barracuda Networks recommends hiding the mail contact from the Global Address List. You can use the following PowerShell command to hide the mail contact:

```
Get-MailContact | Where {$_.Name -eq "Journal Contact"} | Set-MailContact
-HiddenFromAddressListsEnabled $True
```

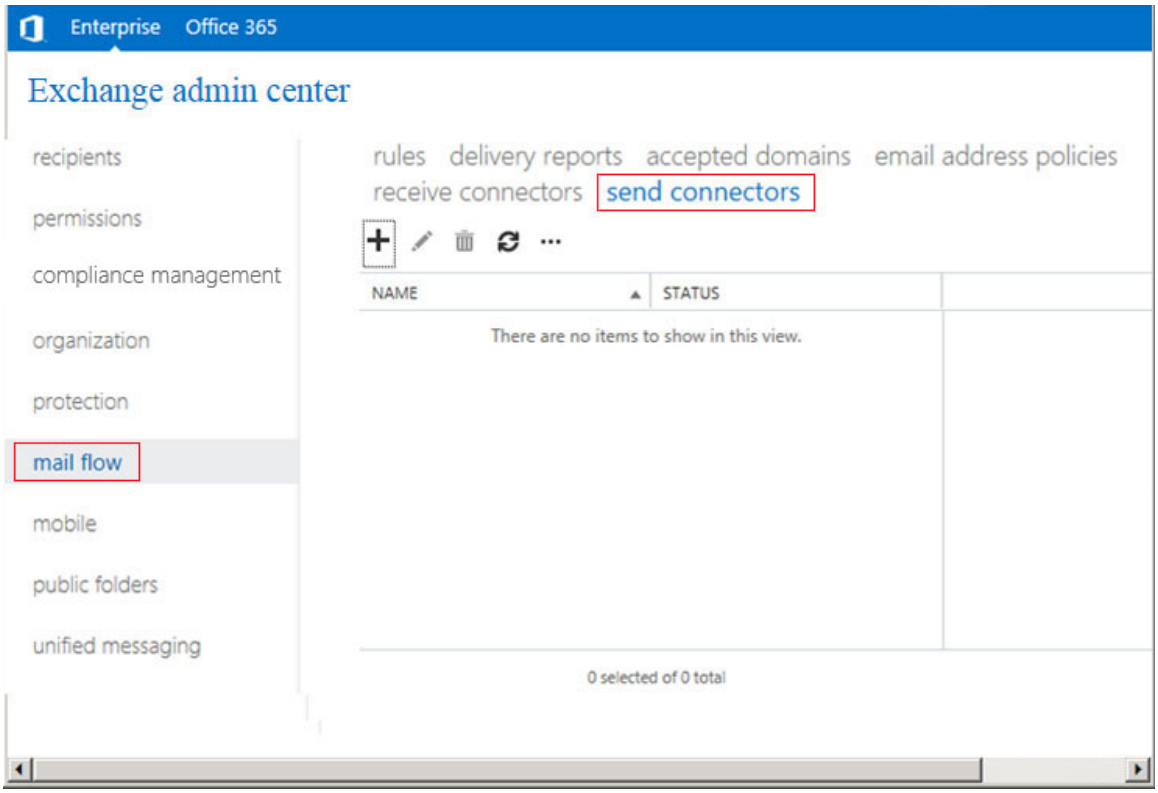
Enter the following command to verify the setting:

```
Get-MailContact | Where {$_.Name -eq "Journal Contact"} | Format-table Name,
HiddenFromAddressListsEnabled
```

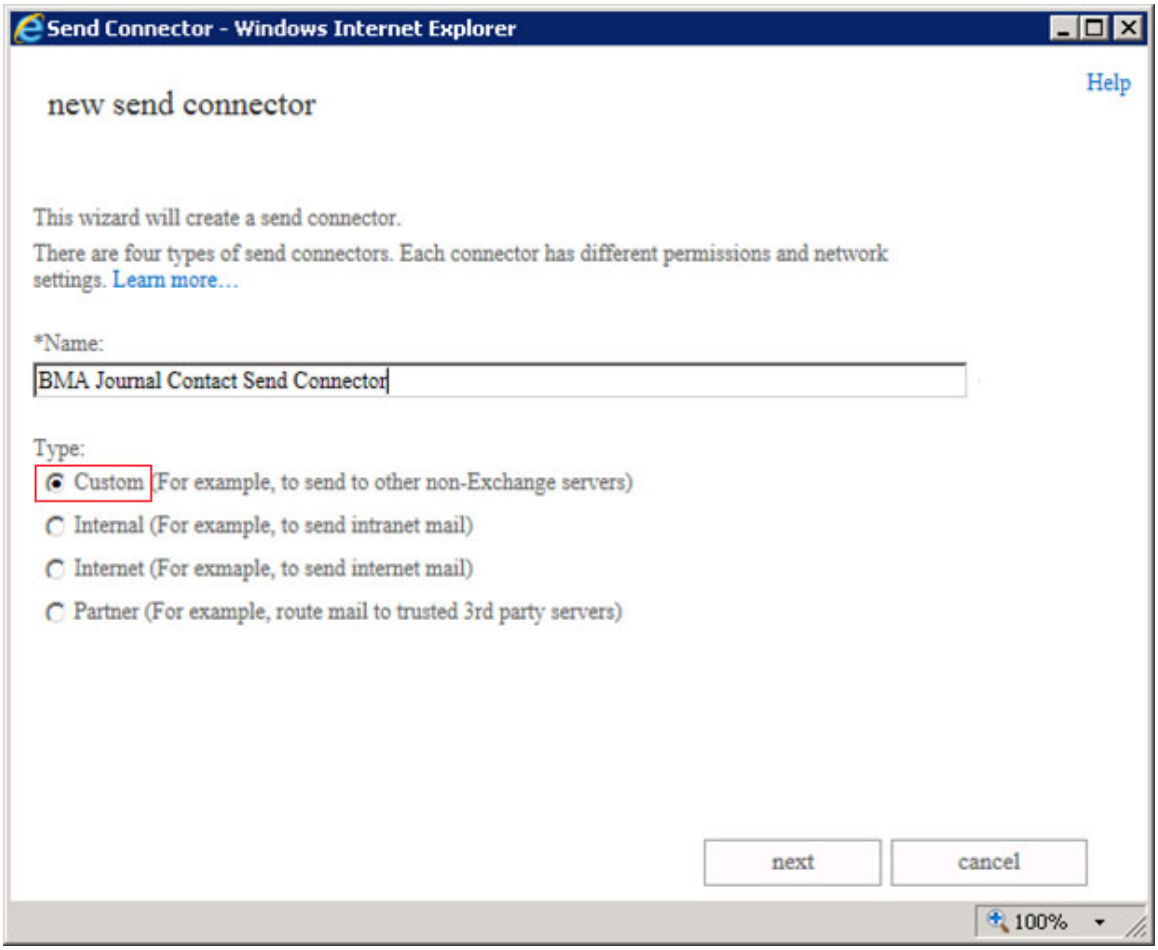
Step 4. Create a Send Connector for the Remote Domain

To route journaled mail that is sent to the contact to the Barracuda Message Archiver, use the following steps to create a Send Connector for the Remote Domain:

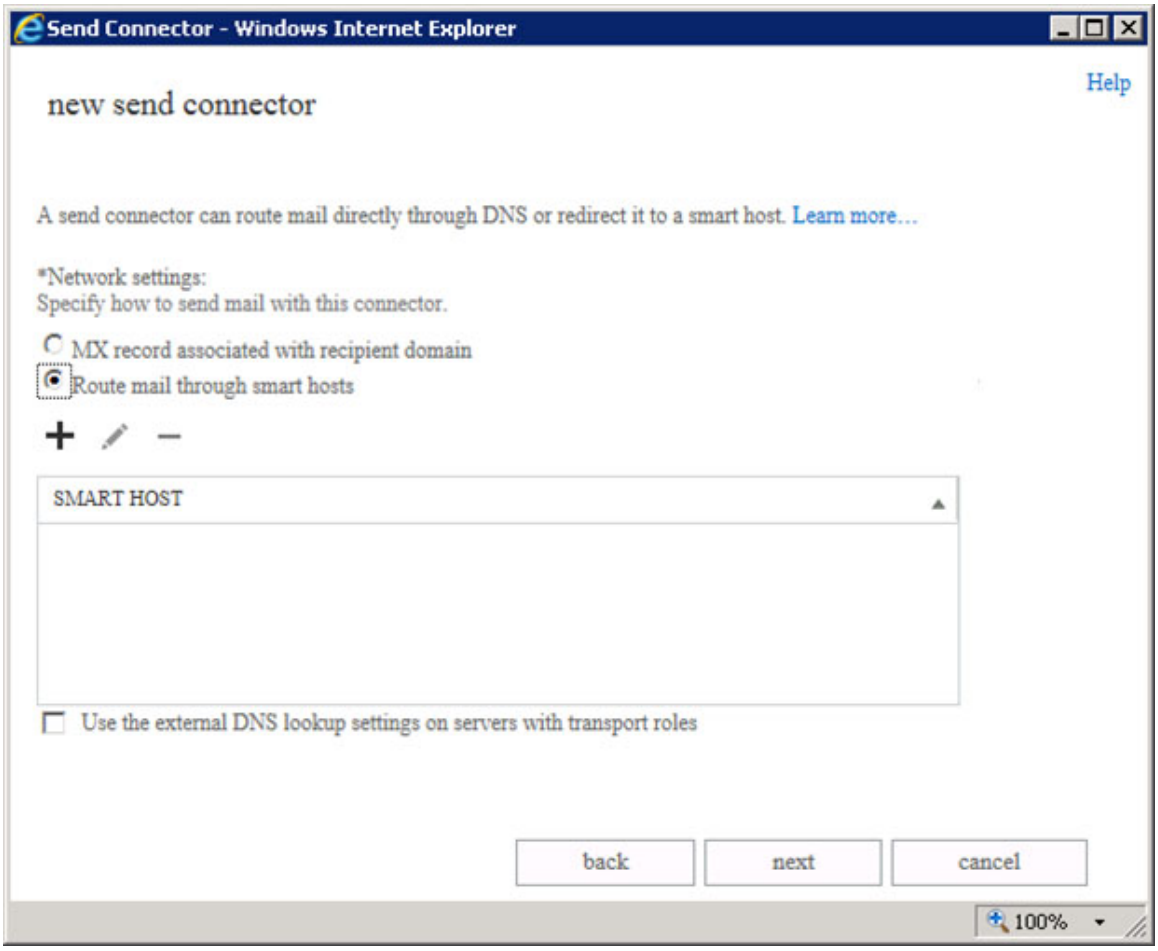
4a. Open Exchange Server 2013, and in the EAC click **mail flow** in the left pane, select **send connectors** at the top of the page, and then click the **Add** (+) icon to create a new send connector:



4b. In the **Name** field, enter a name for the connector, and in the **Type** section, select **Custom**:

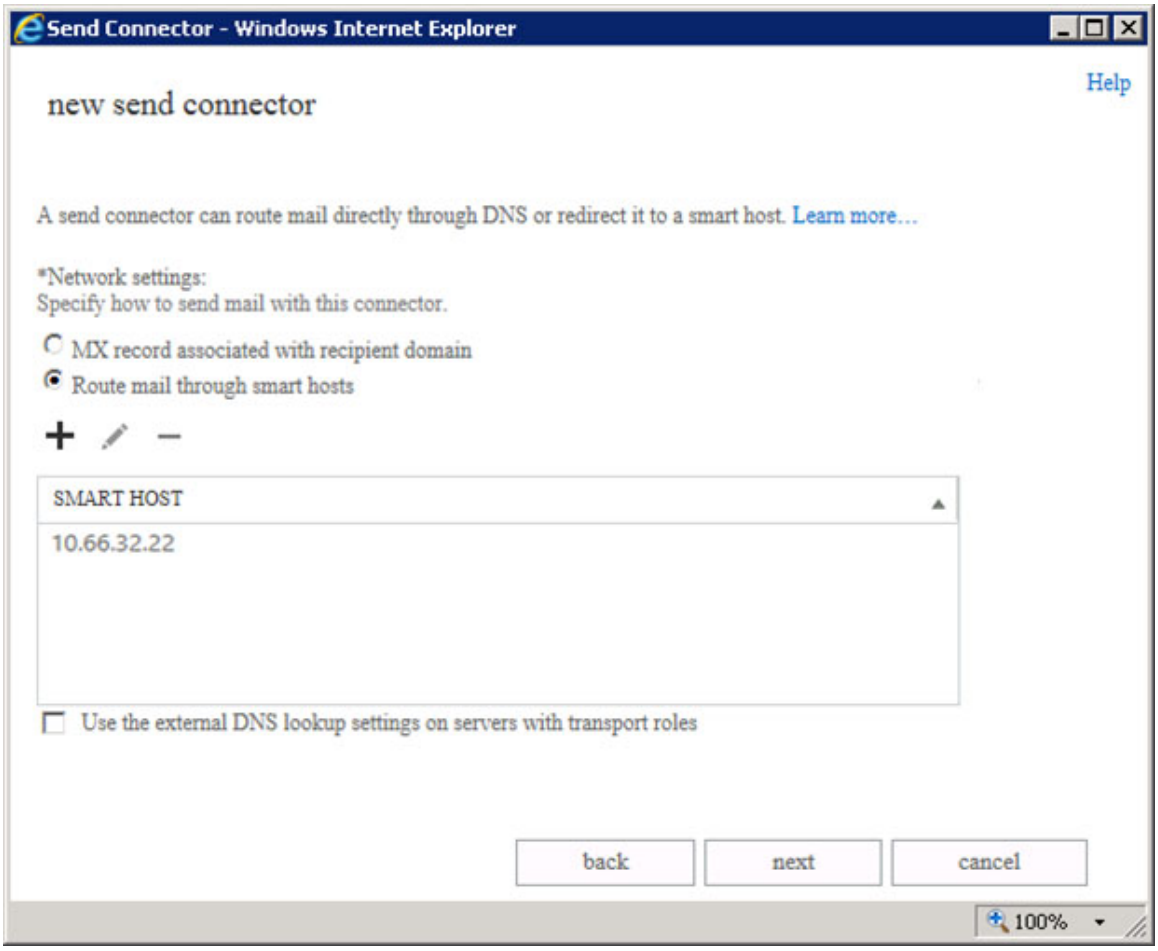

Send Connector - Windows Internet Explorer
new send connector
Help
This wizard will create a send connector.
There are four types of send connectors. Each connector has different permissions and network settings. Learn more...
*Name:
BMA Journal Contact Send Connector
Type:
Custom (For example, to send to other non-Exchange servers)
Internal (For example, to send intranet mail)
Internet (For exmaple, to send internet mail)
Partner (For example, route mail to trusted 3rd party servers)
next
cancel
100%

4c. Click **next**. In the **Network settings** page, select **Route mail through smart hosts**:

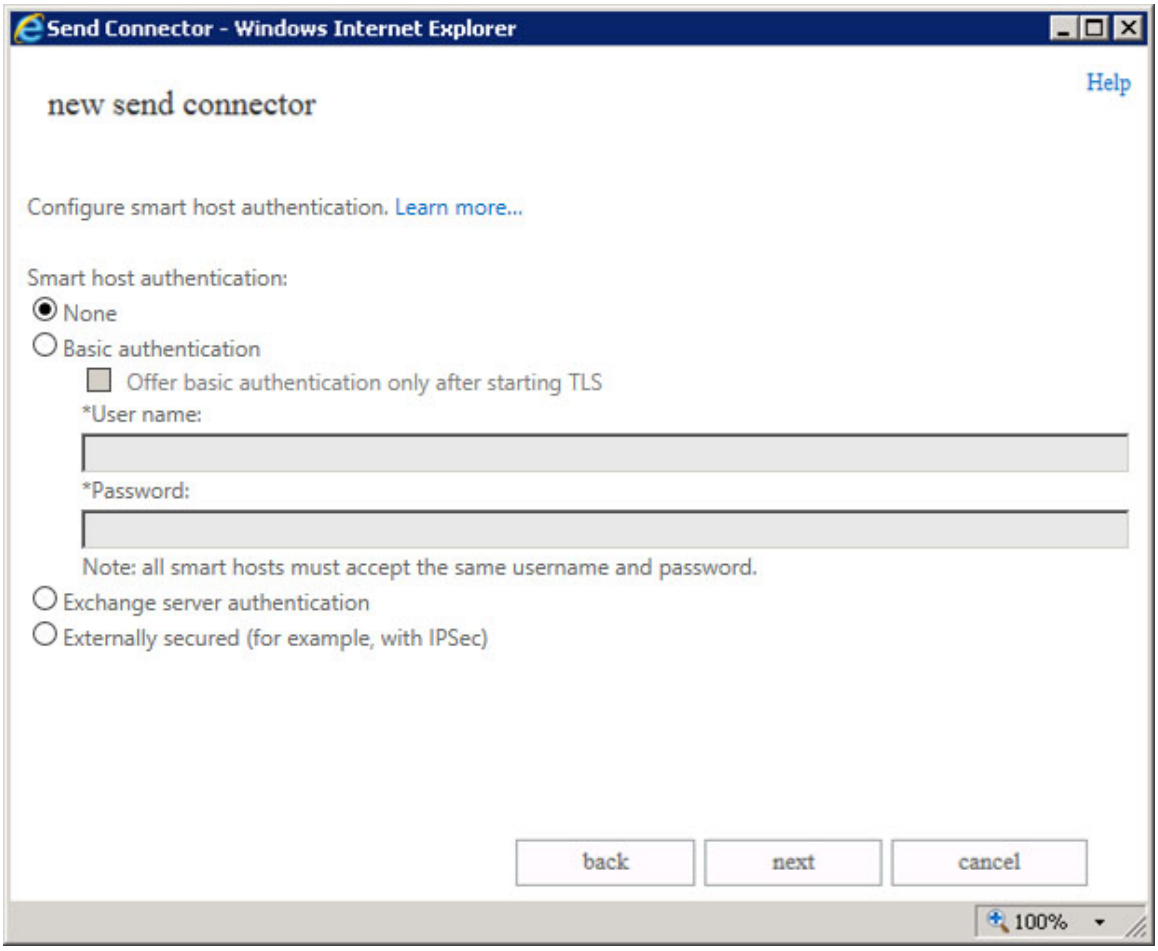

Send Connector - Windows Internet Explorer
Help
new send connector
A send connector can route mail directly through DNS or redirect it to a smart host. Learn more...
*Network settings:
Specify how to send mail with this connector.
MX record associated with recipient domain
Route mail through smart hosts
SMART HOST
Use the external DNS lookup settings on servers with transport roles
back
next
cancel
100%

4d. Click **next**. In the **add smart host** page, enter the fully qualified domain name (FQDN) or IP Address of the Barracuda Message Archiver:

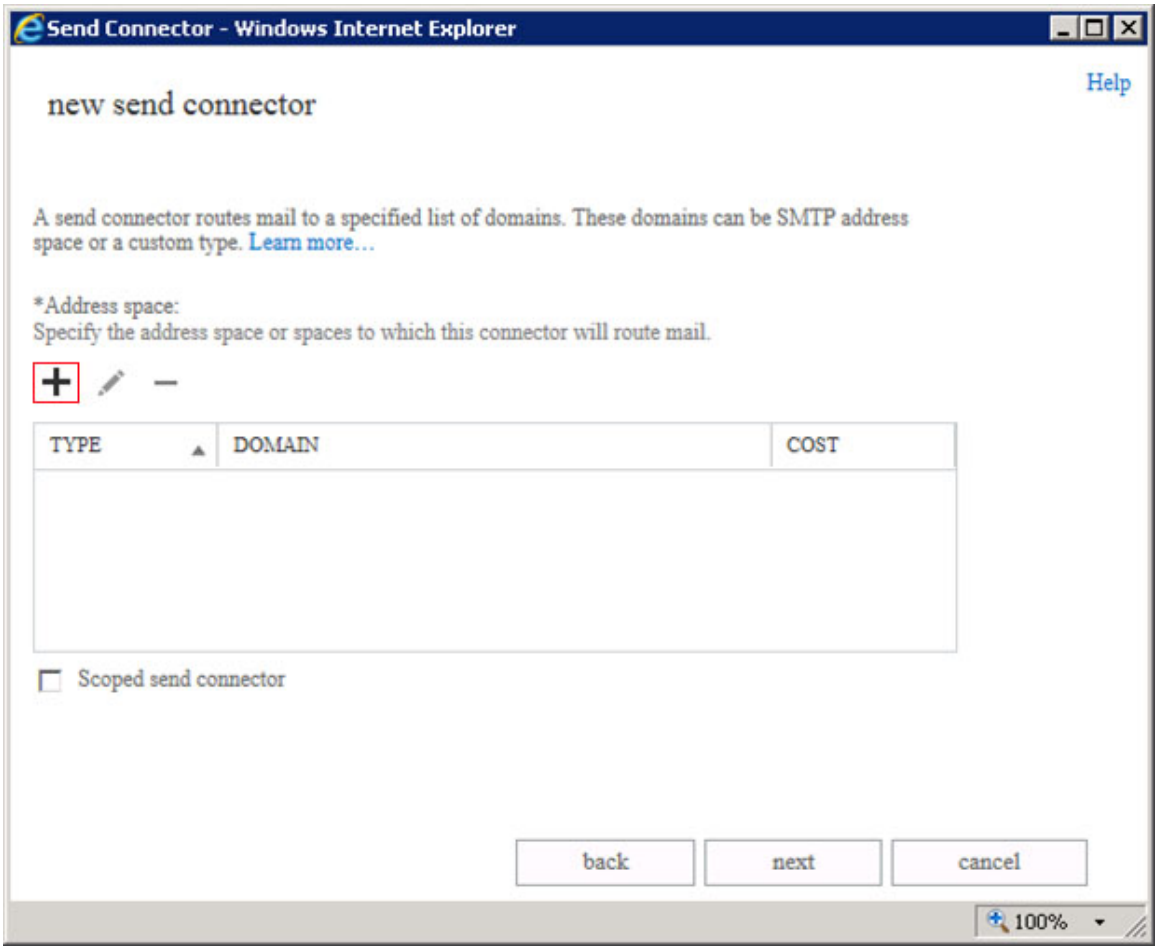
4e. Click **save**. The FQDN or IP Address displays in the **SMART HOST** list; verify the address:


Send Connector - Windows Internet Explorer
Help
new send connector
A send connector can route mail directly through DNS or redirect it to a smart host. Learn more...
*Network settings:
Specify how to send mail with this connector.
MX record associated with recipient domain
Route mail through smart hosts
SMART HOST
10.66.32.22
Use the external DNS lookup settings on servers with transport roles
back
next
cancel
100%

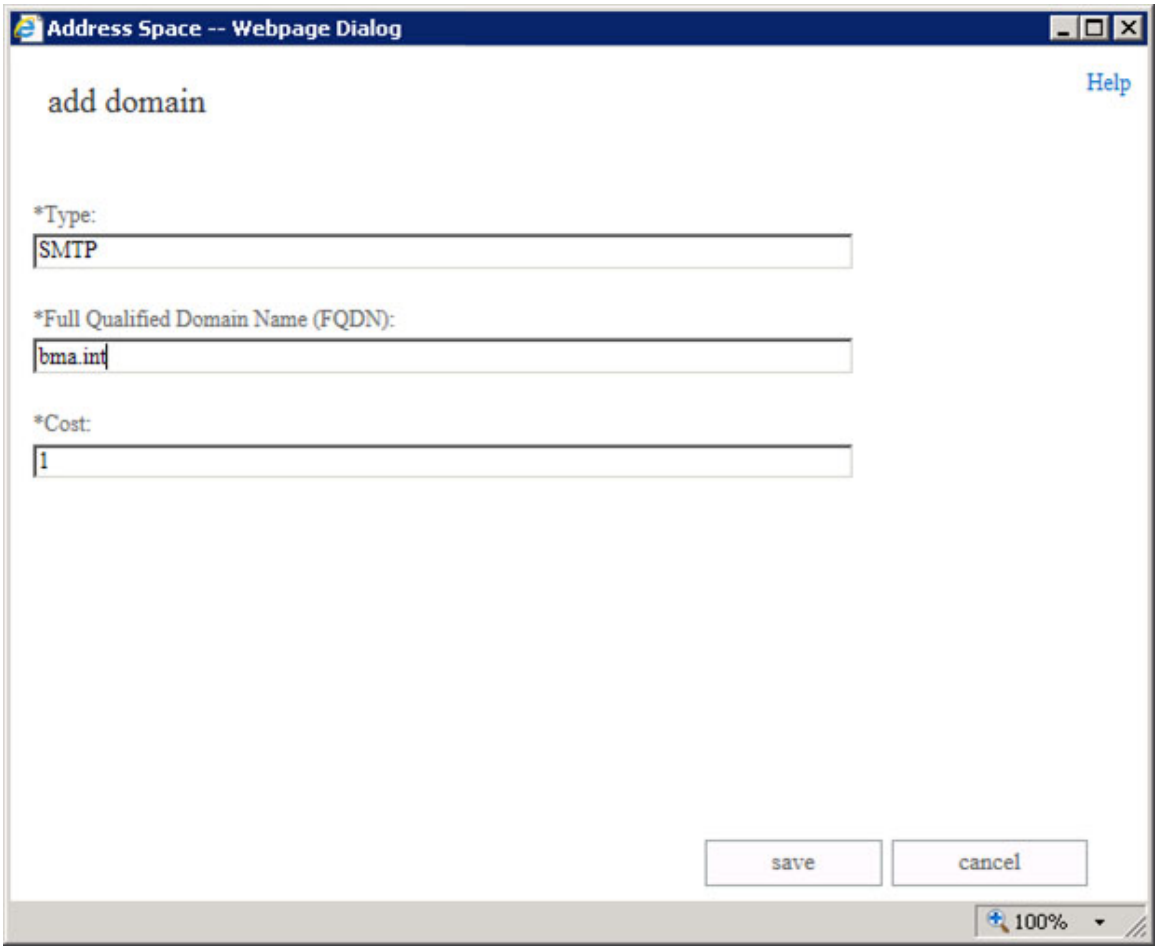
4f. Click **next**. In the **Smart host authentication** page, because authentication is not used on the smart host connection to the Barracuda Message Archiver, no changes are necessary; click **next**:



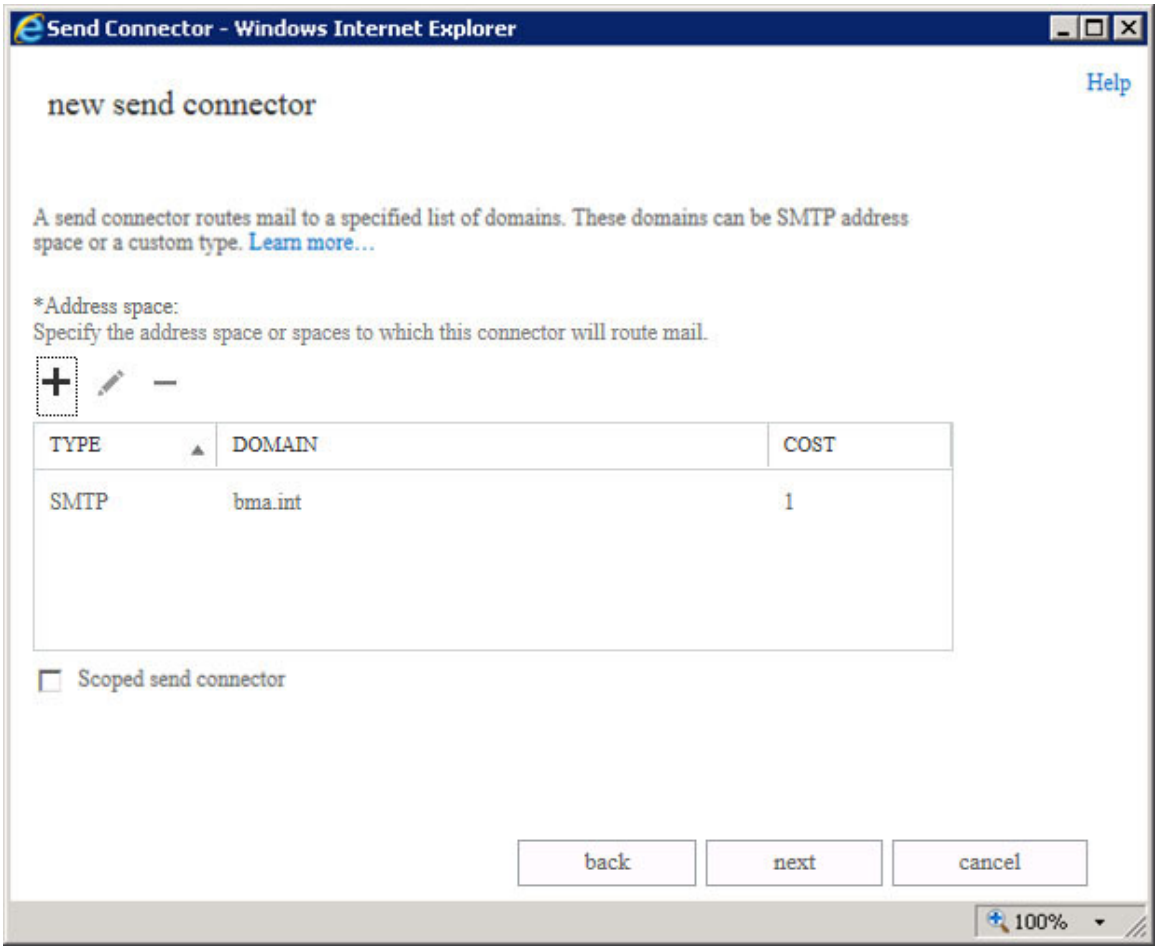
4g. In the **Address space** section, click the **Add** (+) icon:


Send Connector - Windows Internet Explorer
Help
new send connector
A send connector routes mail to a specified list of domains. These domains can be SMTP address space or a custom type. Learn more...
*Address space:
Specify the address space or spaces to which this connector will route mail.
TYPE
DOMAIN
COST
Scoped send connector
back
next
cancel
100%

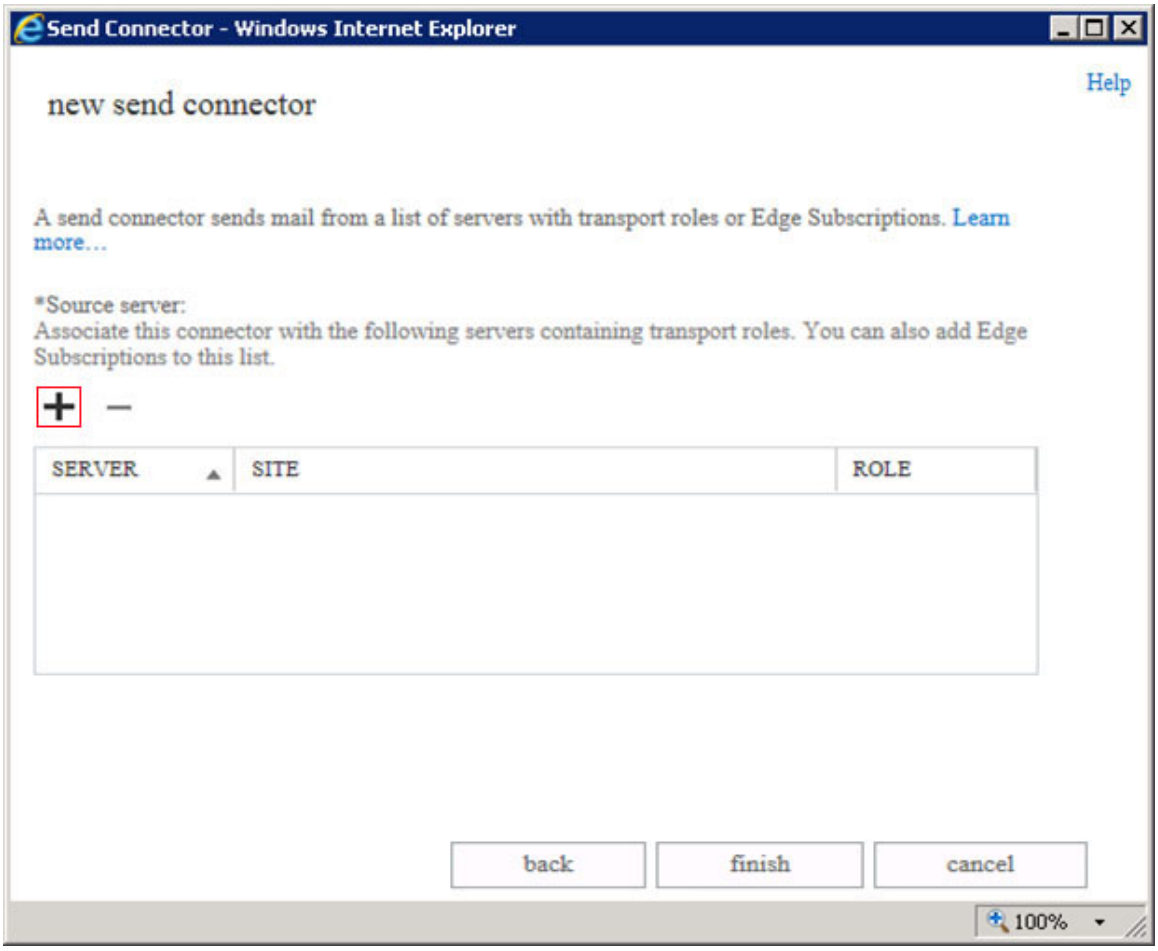
4h. In the **Address Space** page, enter the domain that matches the domain for the external email address used to create the journal contact, for example, `bma.int` (see **Step 2**):



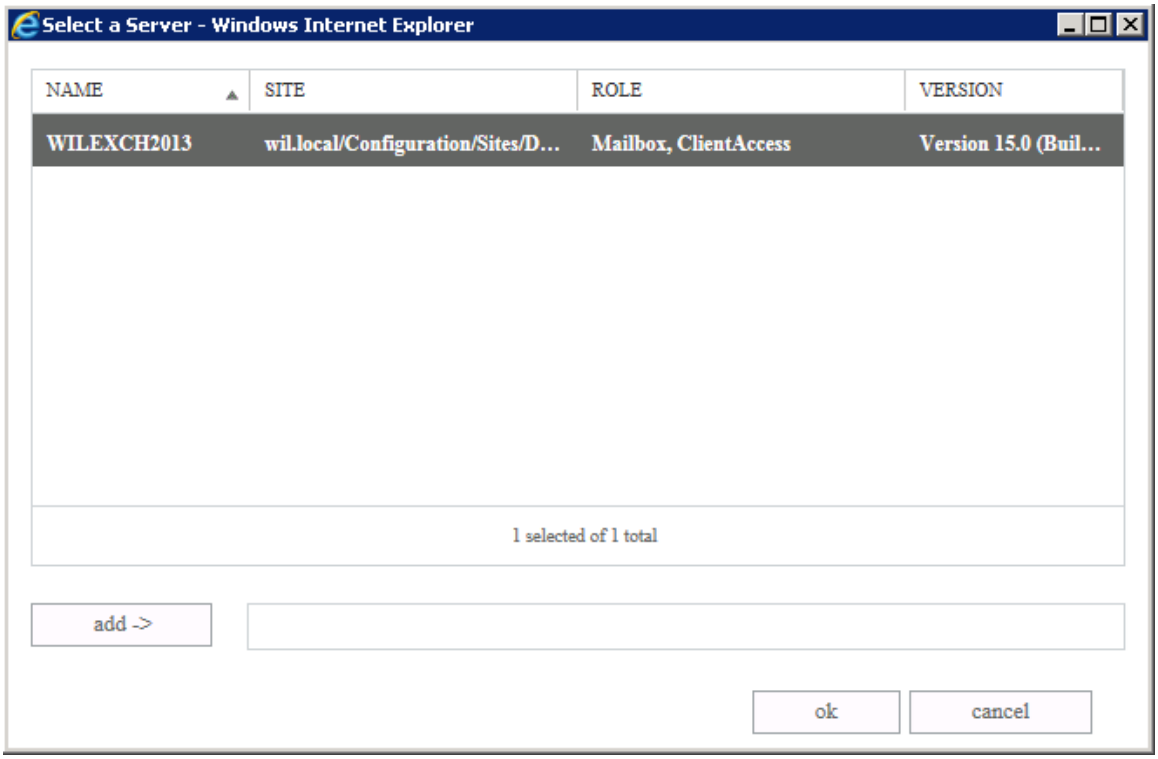
4i. The domain is added to the **Address space** list:



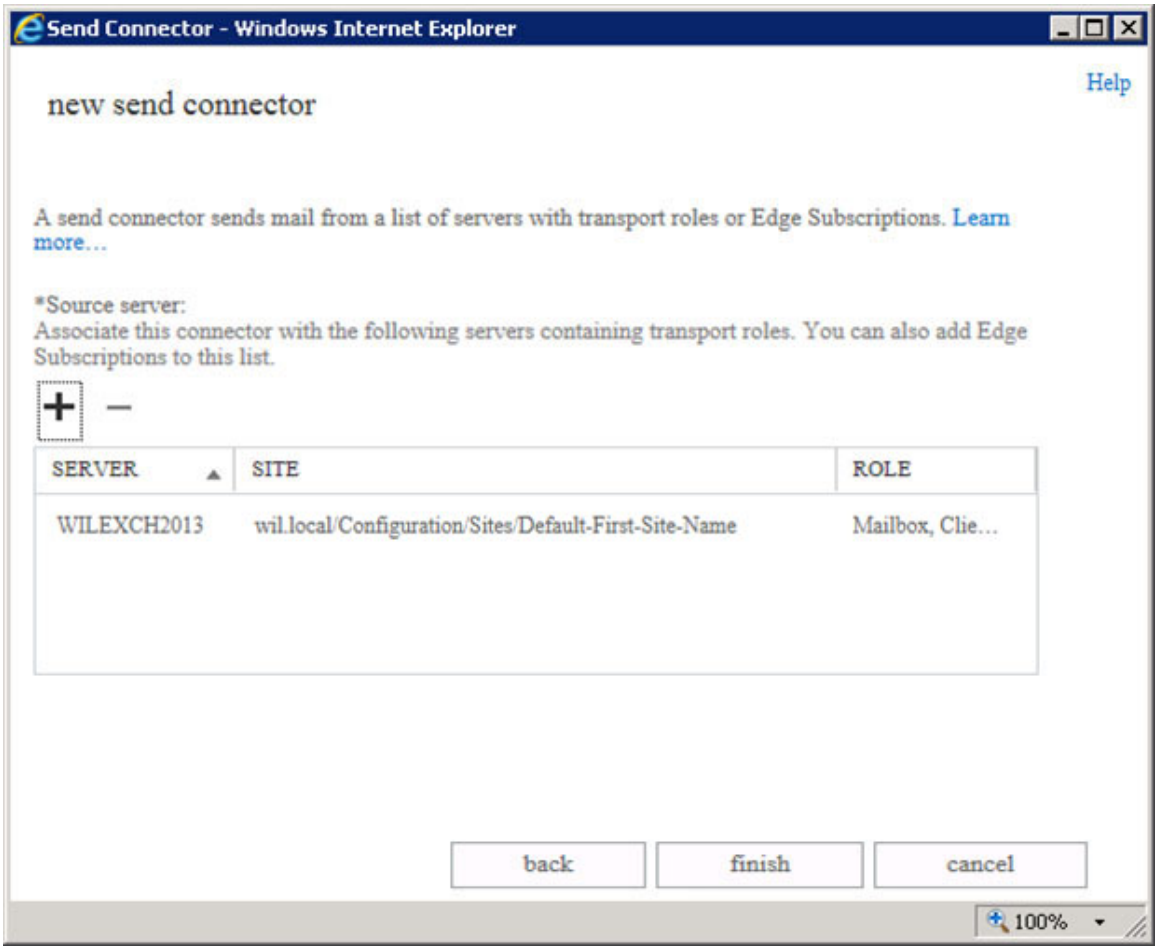
4j. Click **next**. In the **Source server** section, click the **Add** (+) icon:


Send Connector - Windows Internet Explorer
new send connector
Help
A send connector sends mail from a list of servers with transport roles or Edge Subscriptions. Learn more...
*Source server:
Associate this connector with the following servers containing transport roles. You can also add Edge Subscriptions to this list.
SERVER
SITE
ROLE
back
finish
cancel
100%

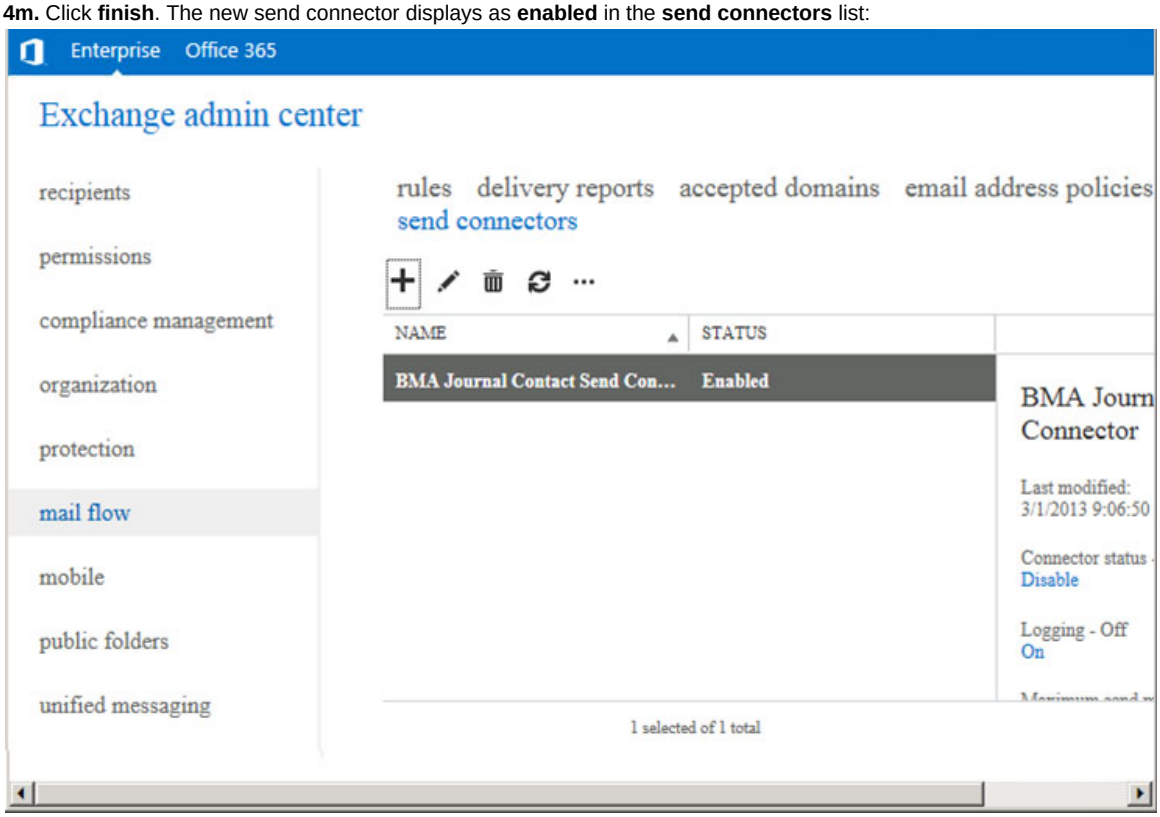
4k. Verify all of the appropriate Exchange Servers are listed; click **add** to add additional servers:



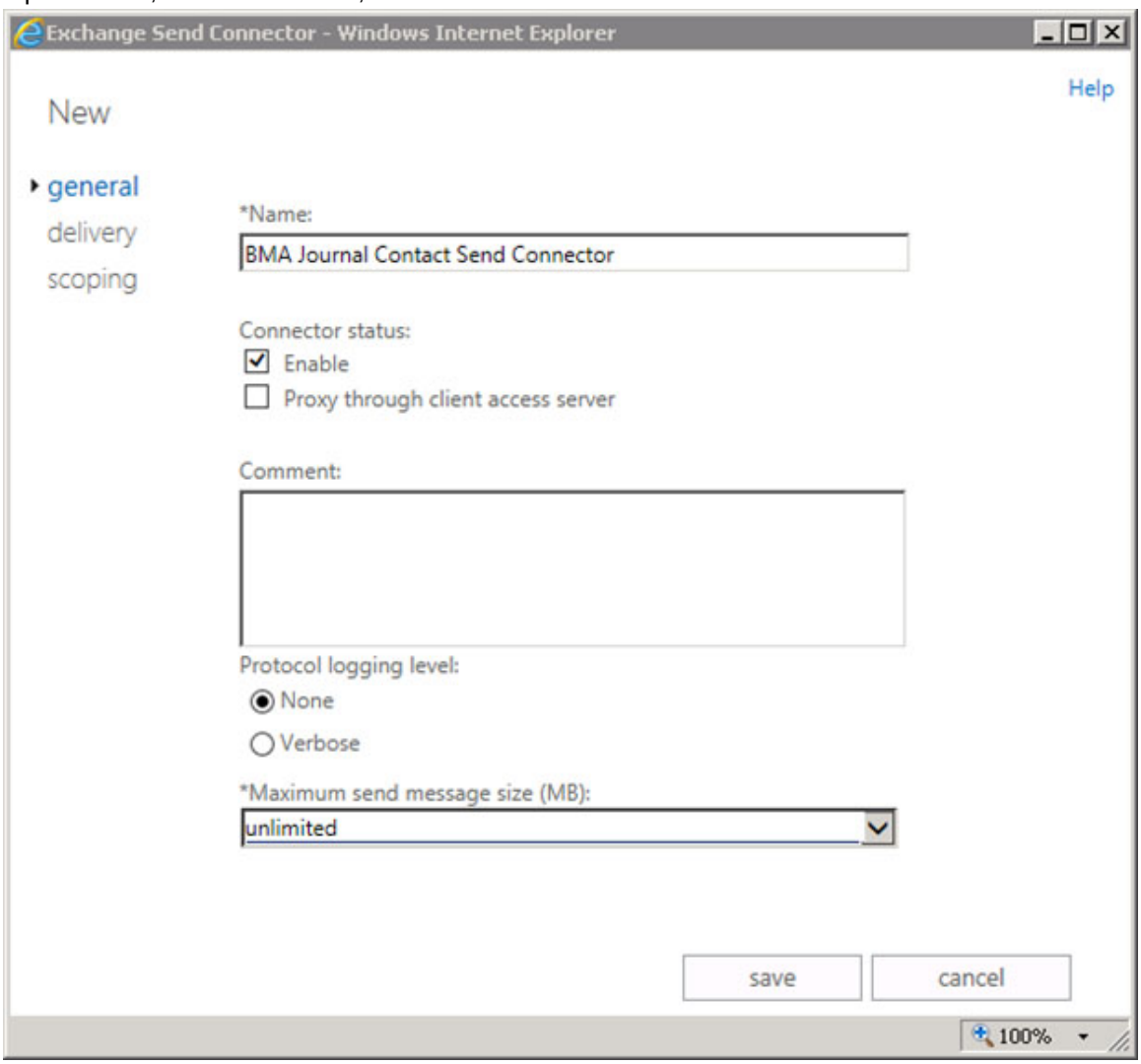
4l. Click **ok**. In the **Source server** page, the selected servers display:



4m. Click **finish**. The new send connector displays as **enabled** in the **send connectors** list:



4n. Click the Edit ( ) icon to edit the Send Connector properties. From the **Maximum send message size (MB)** d rop-down list, select **unlimited**, and then click **save**:



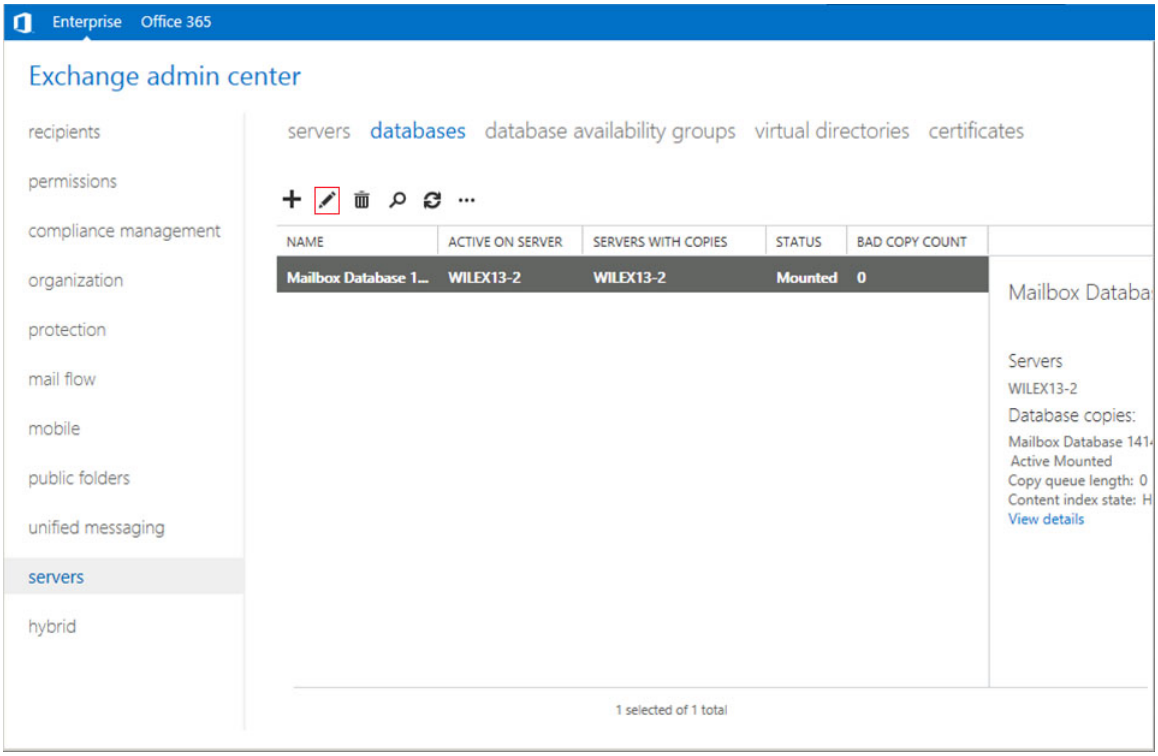
Step 5. Set Up Mailbox Database Journaling

> **Journaling**
> This article assumes you are setting up mailbox database journaling. If you intend to implement a journal rule, refer to the article **How to Configure Envelope (SMTP) Journaling for Microsoft Exchange Server 2013 - Premium Journaling** . Use only *one* journaling method; choose the appropriate method for your environment.

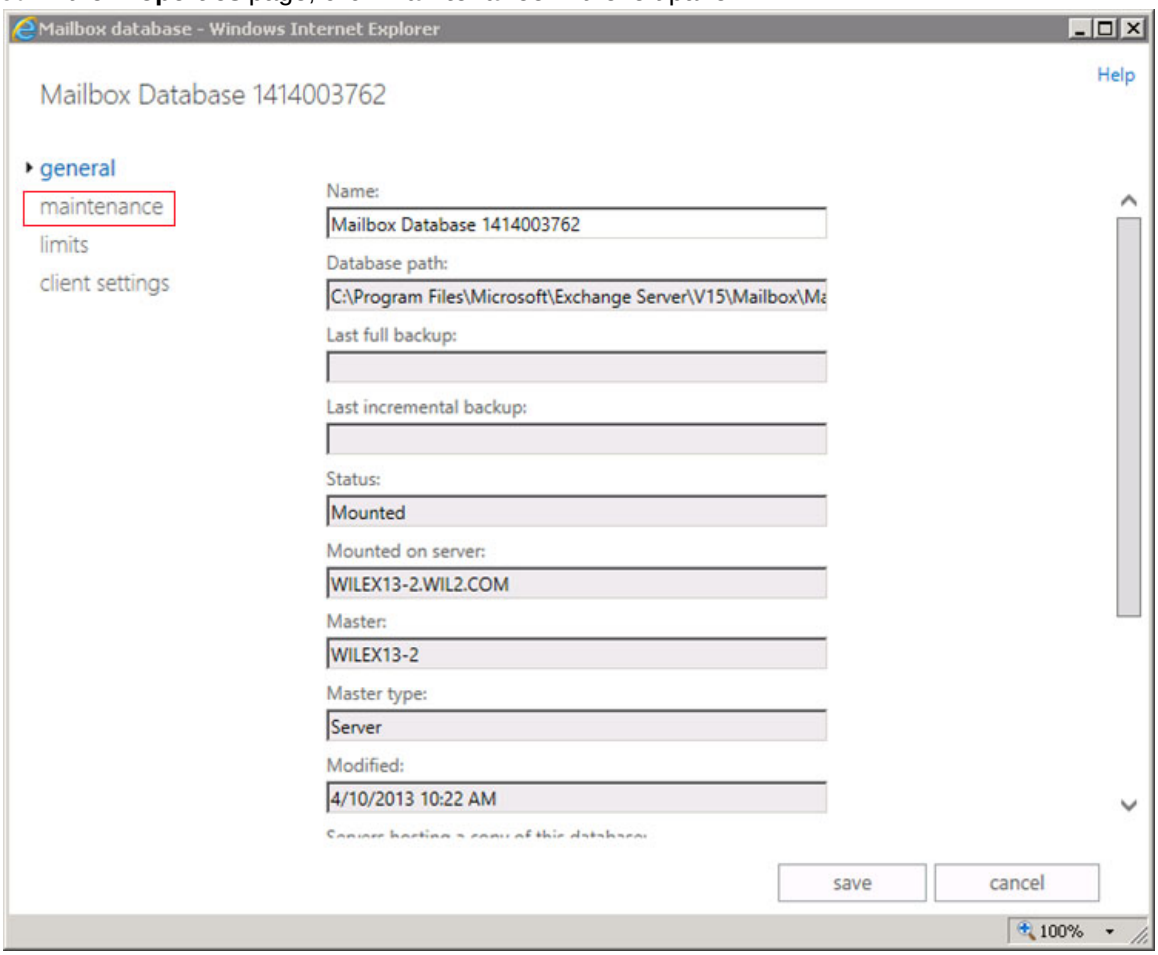
Use the following steps to set up mailbox database journaling:

> **Important**
> You must complete *all* of the steps in this section for *each* Exchange 2013 Email Database.

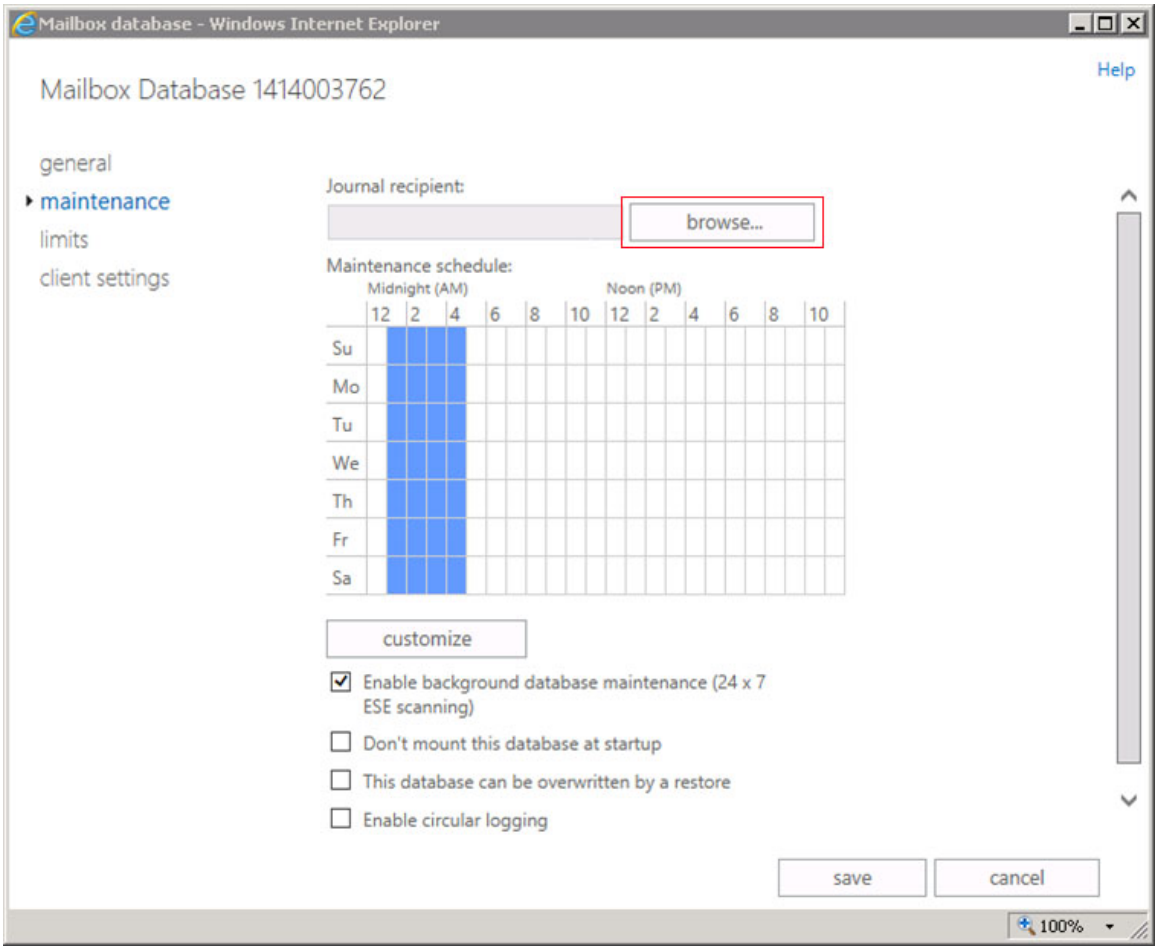
5a. Open Exchange Server 2013, and in the EAC click **servers** in the left pane, select **database** at the top of the page, and then click the Edit ( ) icon to edit the database properties:



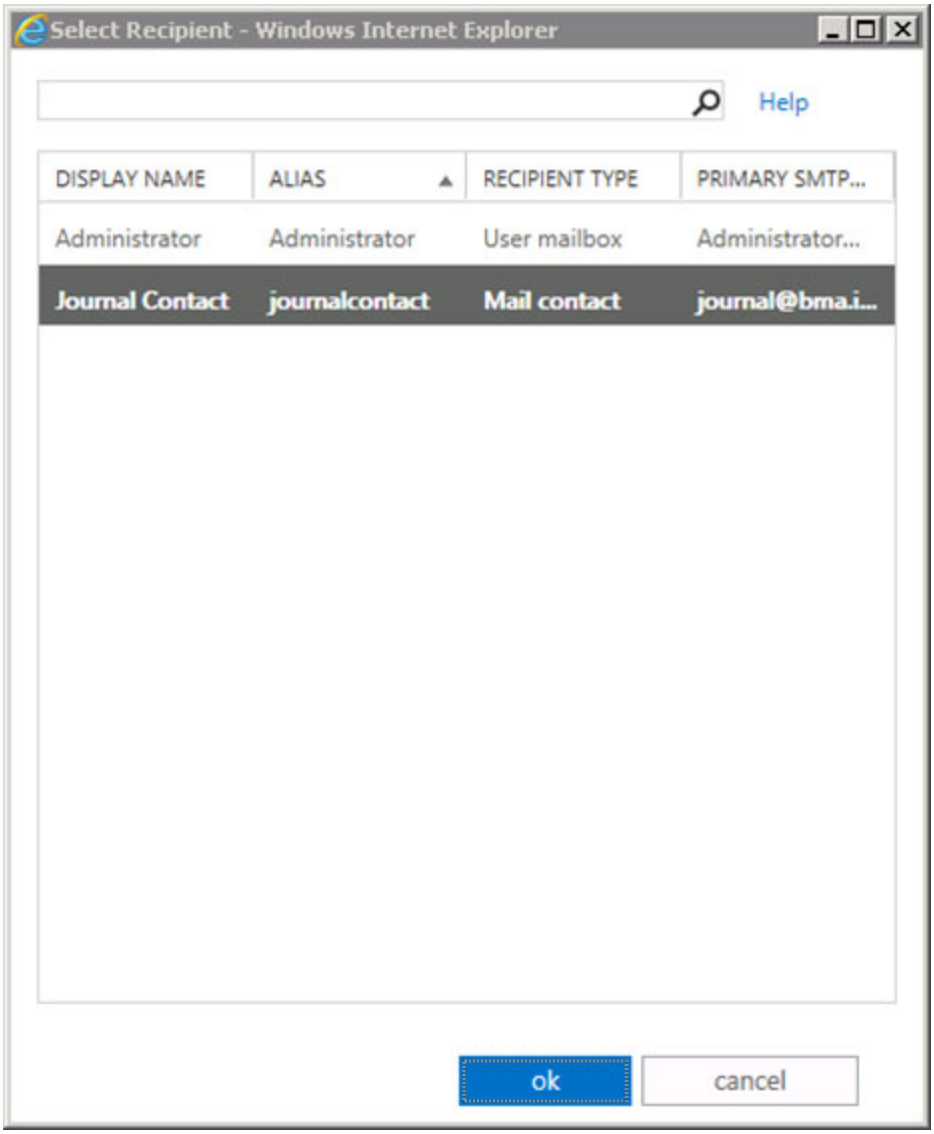
5b. In the **Properties** page, click **maintenance** in the left pane:



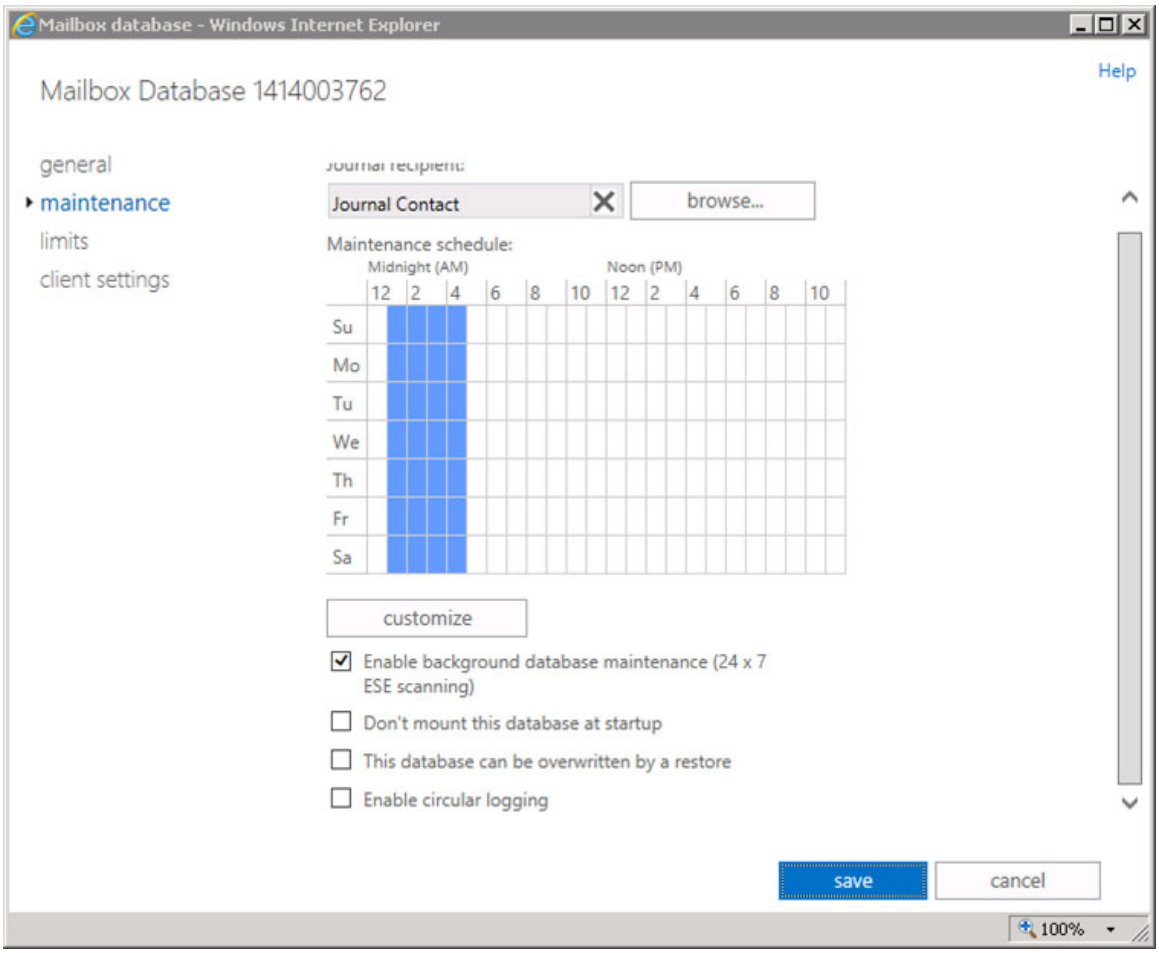
5c. In the **maintenance** page, click **browse** following the **Journal recipient** field:



5d. Navigate to and select the destination location for journaled messages, for example `journal@bma.int`:



5e. Click **ok** to select the journal message recipient. The recipient displays in the **maintenance** page:



5f. Click **save** to save your settings.

The configuration is now complete and journaled mail is forwarded to the Barracuda Message Archiver. Log into the Barracuda Message Archiver, and go to the **BASIC > Search** page in the web interface to verify that new mail is being processed. Note that it may take up to 30 minutes before journaled mail is available in the search results.

Barracuda Networks recommends hiding the Journal Contact–as well as any mailbox set up for undeliverable journal reports–from the Global Address List (GAL) so that mail is not sent directly to these accounts.

How to Configure Envelope (SMTP) Journaling for Microsoft Exchange Server 2013 - Premium Journaling

This article refers to the Barracuda Message Archiver firmware version 3.2 and higher, and a Microsoft® Exchange Server 2013 environment utilizing Premium Journaling with a Journal Rule and Exchange Enterprise Client Access Licenses (CALs).

If your Exchange environment *does not support* Premium Journaling, see the article How to Configure Envelope (SMTP) Journaling for Microsoft Exchange Server 2013 - Standard Journaling.

Microsoft Exchange allows a Journal recipient to be either a *mailbox* or *contact*. By using a contact with an email address that is part of a non-existent domain, you can create a send connector that uses SMTP to deliver journaled mail to the Barracuda Message Archiver.

In this article:

- Step 1. Register Each Exchange Server as a Trusted SMTP Server

- Step 2. Create a Remote Domain From the Exchange Management PowerShell
- Step 3. Create a Recipient Mail Contact/Alternate Email Address
- Step 4. Create a Send Connector for the Remote Domain
- Step 5. Create a Journal Rule

Related Articles

- Understanding SMTP Forwarding and Trusted Servers

Full support for Exchange integration is available in Barracuda Message Archiver firmware version 3.5 or higher; support for Exchange Server 2013 Journaling is available in release 3.1 or higher. Mail sources/Exchange integration features for Exchange Server 2013 are available in firmware version 3.5 or higher.

Use the examples included in this article to simplify troubleshooting. Note that you can cut and paste the shell commands directly from this article.

Step 1. Register Each Exchange Server as a Trusted SMTP Server

To ensure that archiving begins as soon as your Exchange Servers are configured to send journal copies, first register each Exchange Server that is in a Client Access Server (CAS) role as a Trusted SMTP Server with the Barracuda Message Archiver on the **MAIL SOURCES** > **SMTP/IM** page in the web interface.

1a. Log into the Barracuda Message Archiver web interface, and go to the **MAIL SOURCES > SMTP/IM** page.

1b. In the **Trust SMTP Servers** section, enter the details for each Exchange Server that is to journal directly to the Barracuda Message Archiver; click **Add** after entering the details for each Exchange Server, and then click **Save Changes**.

Step 2. Create a Remote Domain From the Exchange Management PowerShell

The Remote Domain must NOT be your normal email domain. The remote domain must be a non-existent and non-routable/unresolvable domain from either inside or outside your organization (such as `bma.int`). This domain must be used for the email address of the Mail Contact that is to be the journaled message recipient.

Remote Domain
In previous versions of Exchange Server, the Exchange Management Console was used to create a Remote Domain; in Exchange Server 2013 the ECP/EAC has no analogous functionality so you must use PowerShell to create the Remote Domain.

To create a Remote Domain, you must enter a **Name** to describe the domain, and the actual **Domain Name** to use. In this example, `bma.int` is the "fake" Domain Name that is used. You can use `bma.int` or create your own "fake" Domain Name. Note that this Domain Name is used when creating the **Mail Contact** in **Step 4**.

2a. Open Exchange Server 2013, and click **Exchange Management Shell**.

2b. Execute the following command to create the remote domain; this command ensures TNEF encloding is disabled and auto-forwarding is enabled:

```
New-RemoteDomain -DomainName bma.int -Name "Message Archiver Domain"

Get-RemoteDomain | Where {$_.DomainName -eq "bma.int"} | Set-RemoteDomain -TNEFEnabled $false
-AutoForwardEnabled $true
```

2c. Enter the following command to verify the settings:

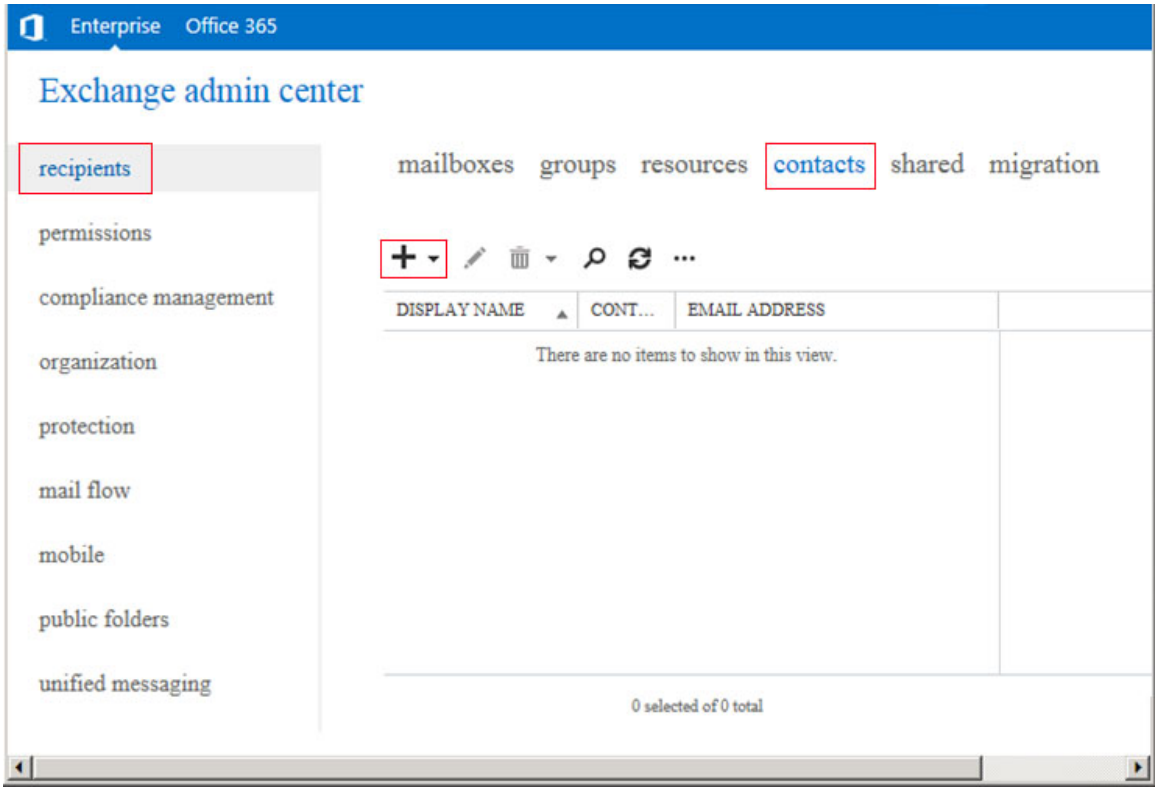
```
Get-RemoteDomain | Where {$_.DomainName -eq "bma.int"} |Format-table Name, DomainName, TNEFEnabled,
AutoForwardEnabled
```

This command ensures TNEF encoding is disabled and auto-forwarding is enabled. Barracuda recommends disabling TNEF encoding. Auto-forwarding is enabled to allow mail for the contact to be forwarded to the Barracuda Message Archiver.

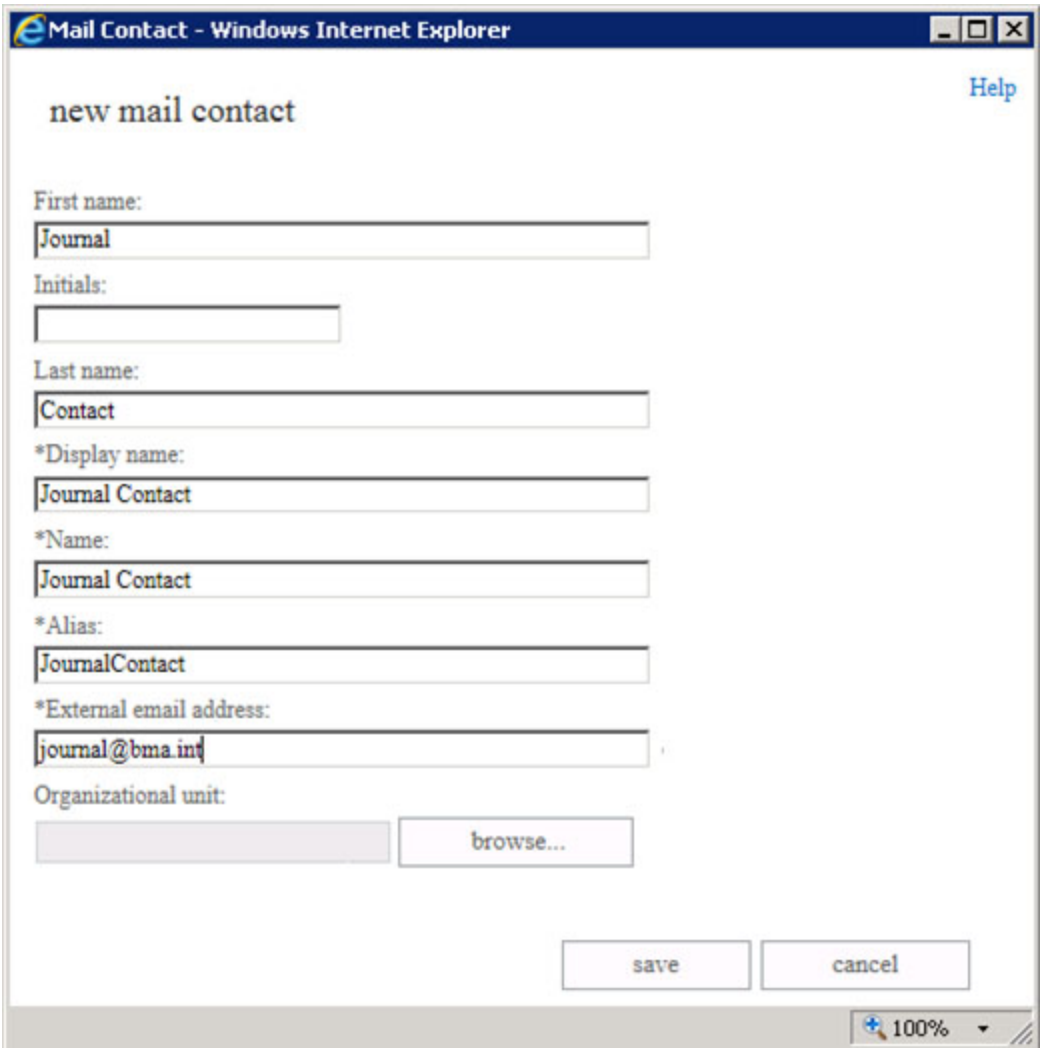
Step 3. Create a Recipient Mail Contact/Alternate Email Address

The Mail Contact is the account that is to act as a "holding location" for journaled messages. The email address associated with this account is the designated recipient and must be associated with a non-existent, non-routable dummy Domain Name created above in **Step 2**. Use the following steps to create the Mail Contact:

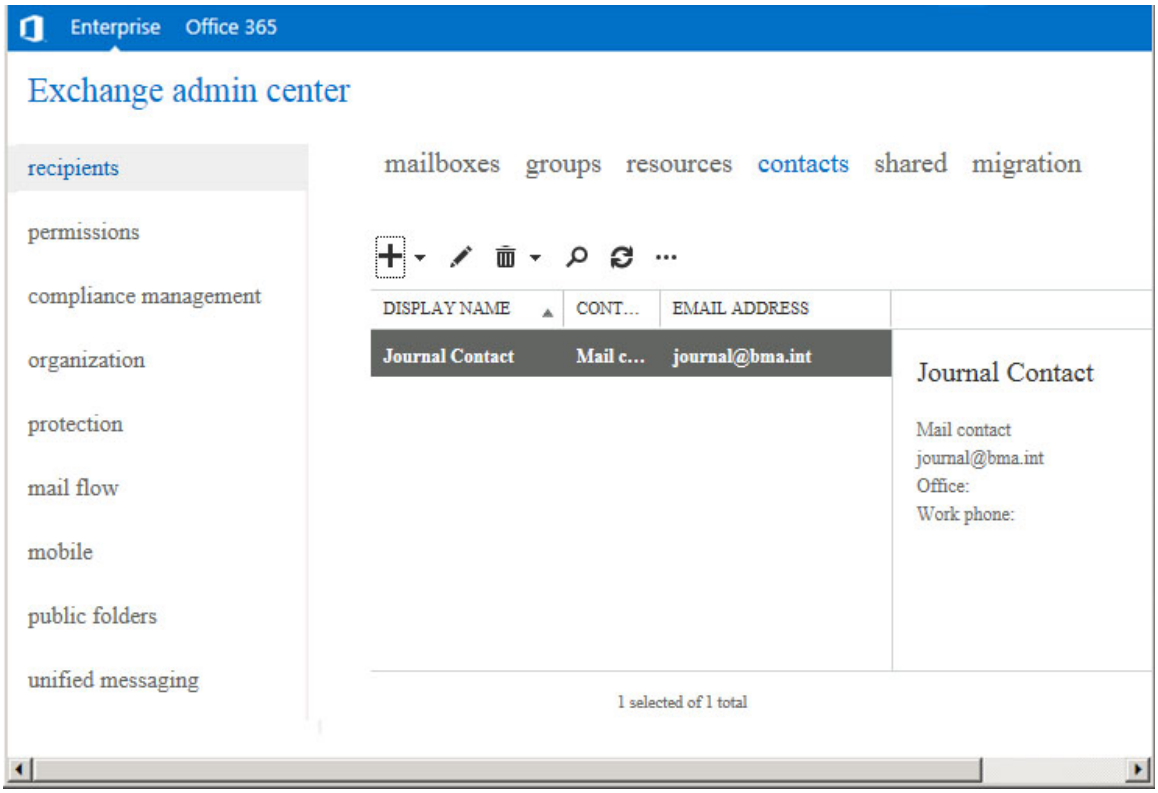
3a. Open Exchange Server 2013, and in the Exchange Admin Center (EAC) click **recipients** in the left pane, select **contacts** at the top of the page, and then click the **Add** (+) icon to create a new mail contact:



3b. In the **new mail contact** page, enter details for the designated recipient account details:



3c. Click **save**. The new contact displays in the **contacts** list:



Hide Contact from Global Address List

Barracuda Networks recommends hiding the mail contact from the Global Address List (GAL). One method to hide the mail contact is to utilize the following shell command:

```
Get-MailContact | Where {$_.Name -eq "Journal Contact"} | Set-MailContact
-HiddenFromAddressListsEnabled $True
```

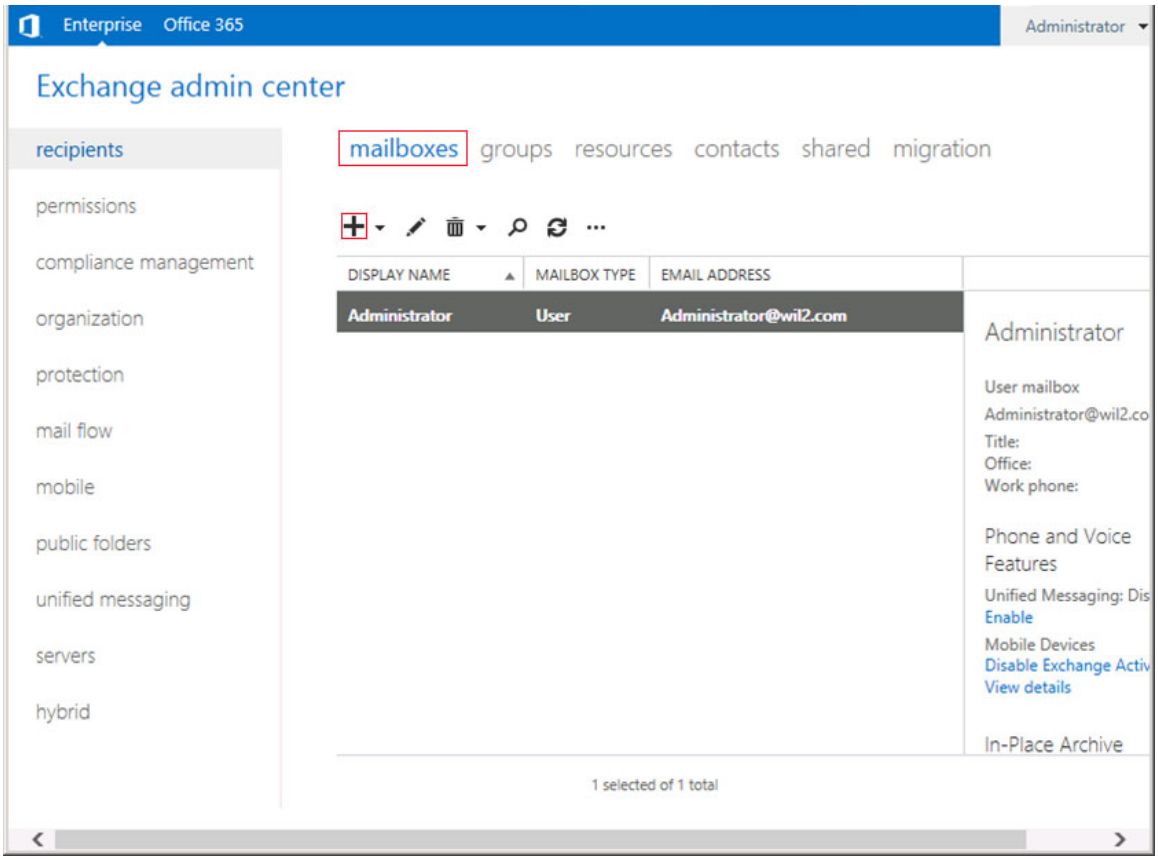
The setting can be verified by executing:

```
Get-MailContact | Where {$_.Name -eq "Journal Contact"} | Format-table Name,
HiddenFromAddressListsEnabled
```

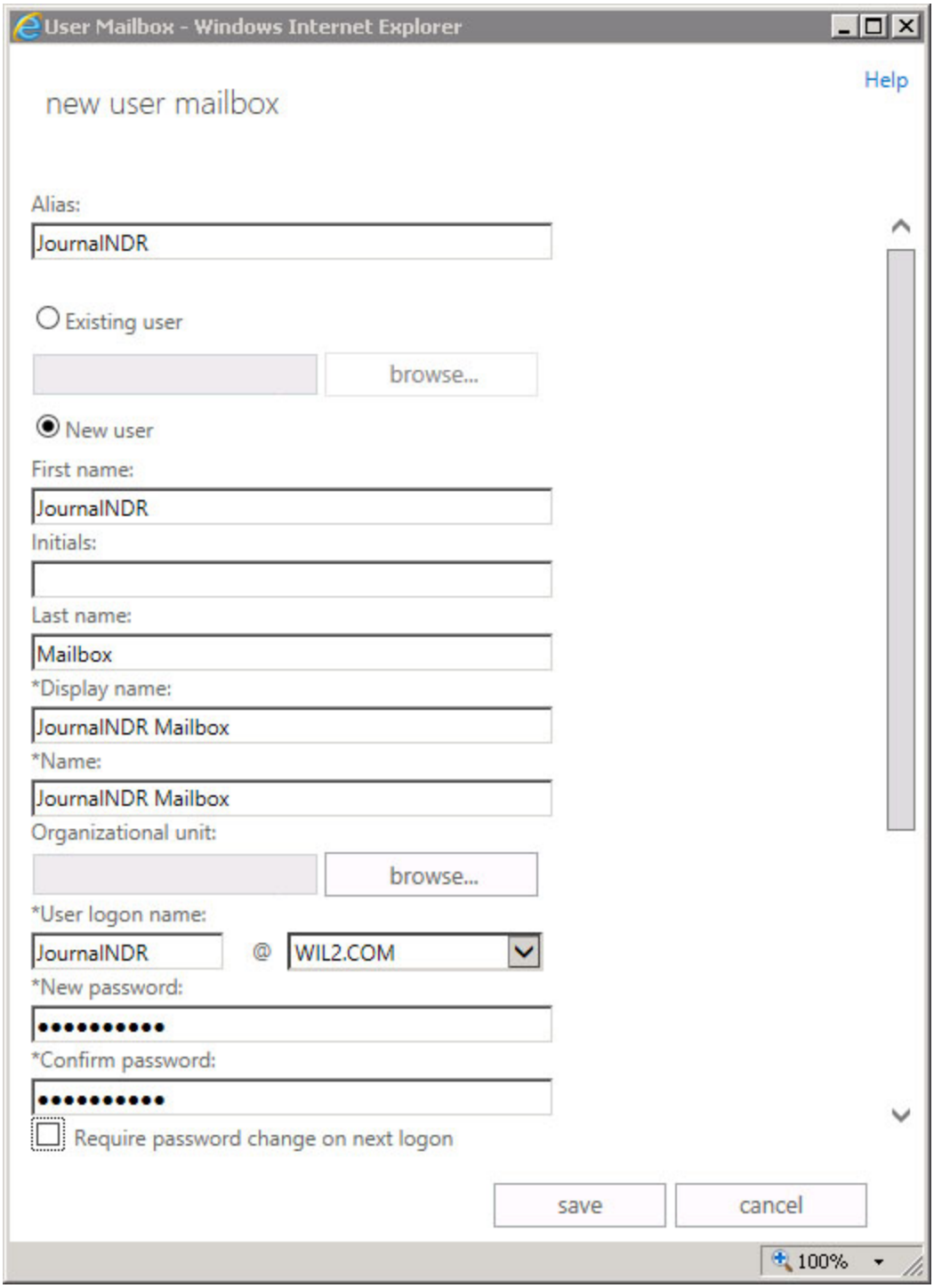
Alternate Journaling Mailbox

You can configure an additional parameter in Exchange 2013 to specify that a journal report temporarily cannot be delivered. For details, refer to the Journal Reports section of the Microsoft TechNet **Journaling** article.

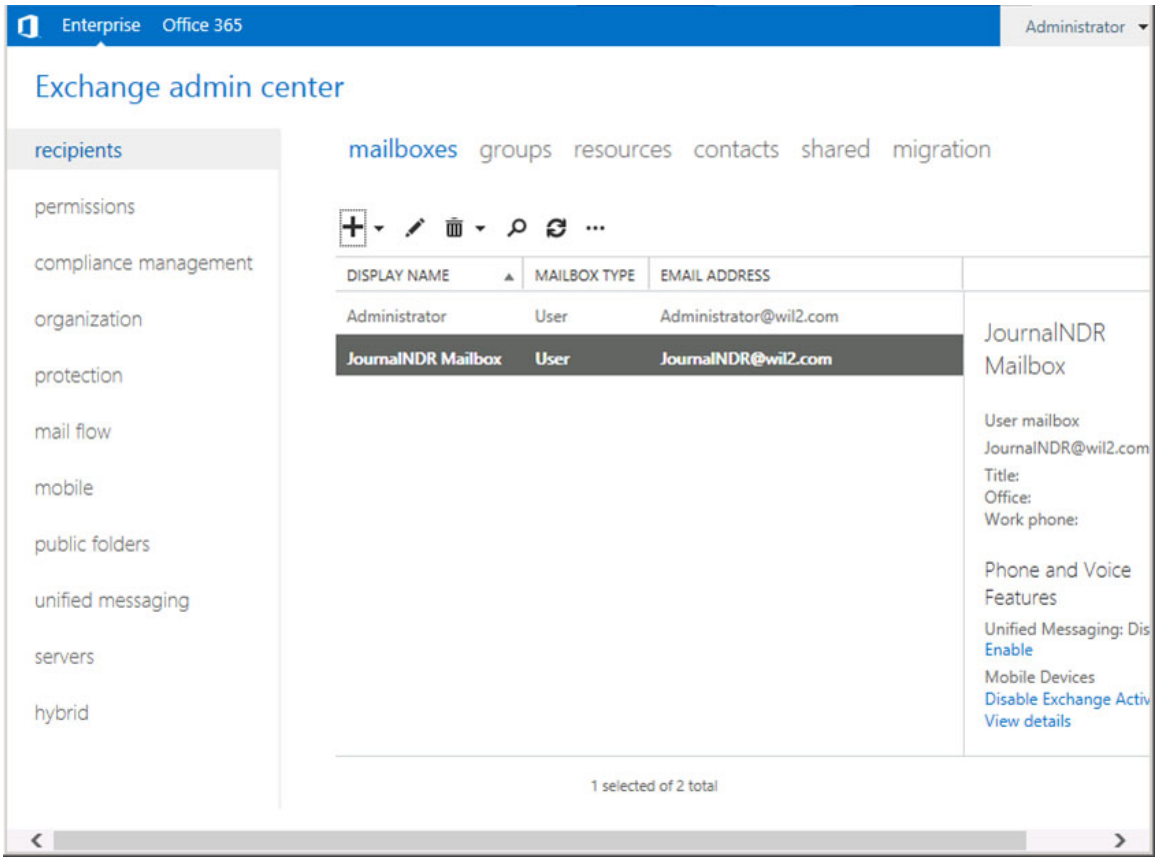
3d. In the EAC, click **recipients** in the left pane, select **mailboxes** at the top of the page, and then click the **Add** (+) icon to create an alternate journaling mailbox:



3e. In the **new user mailbox** page, enter details for the alternate journaling mailbox:

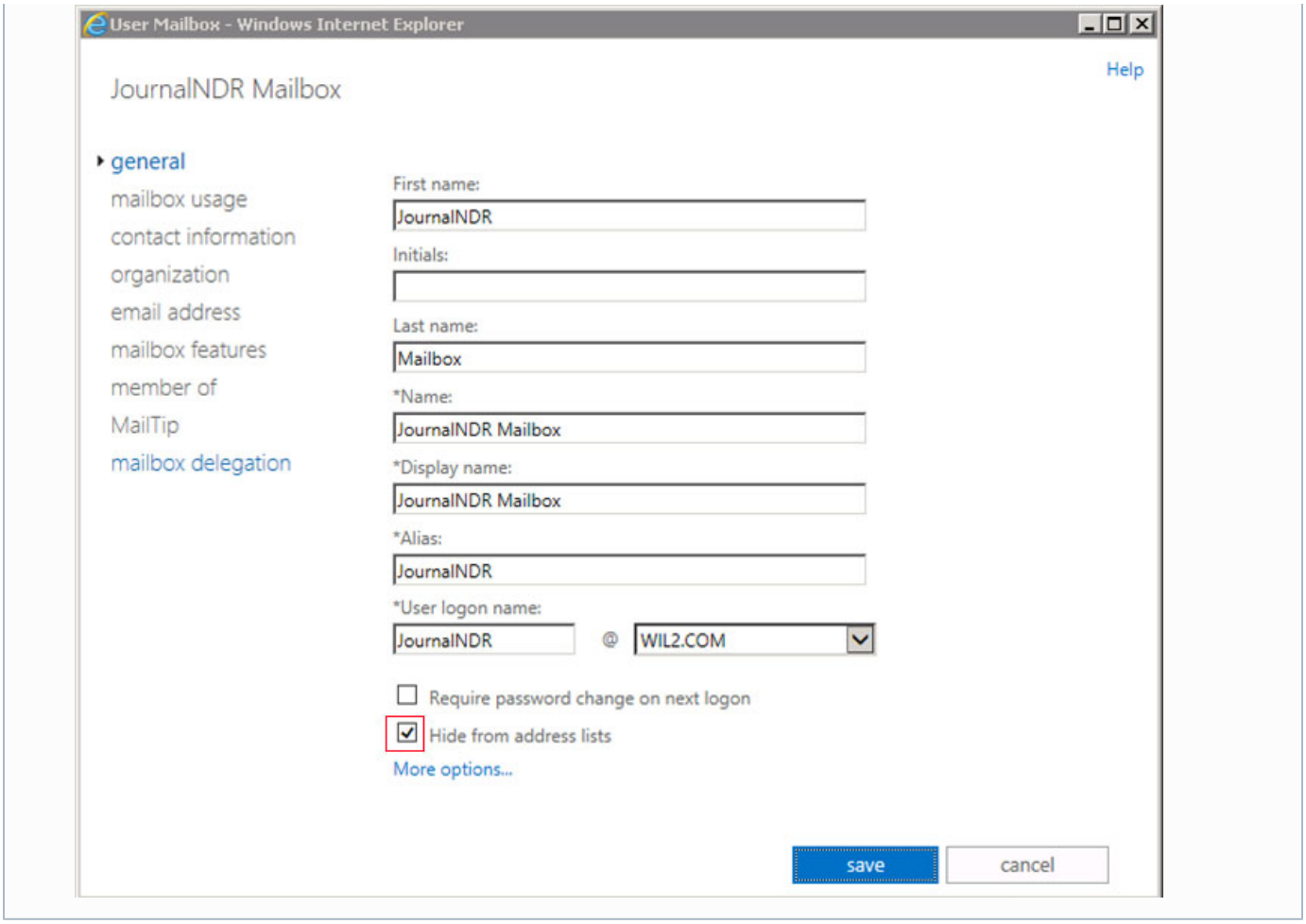


3f. Click **save** The new mailbox displays in the **mailboxes** list:



Hide Alternate Contact from GAL

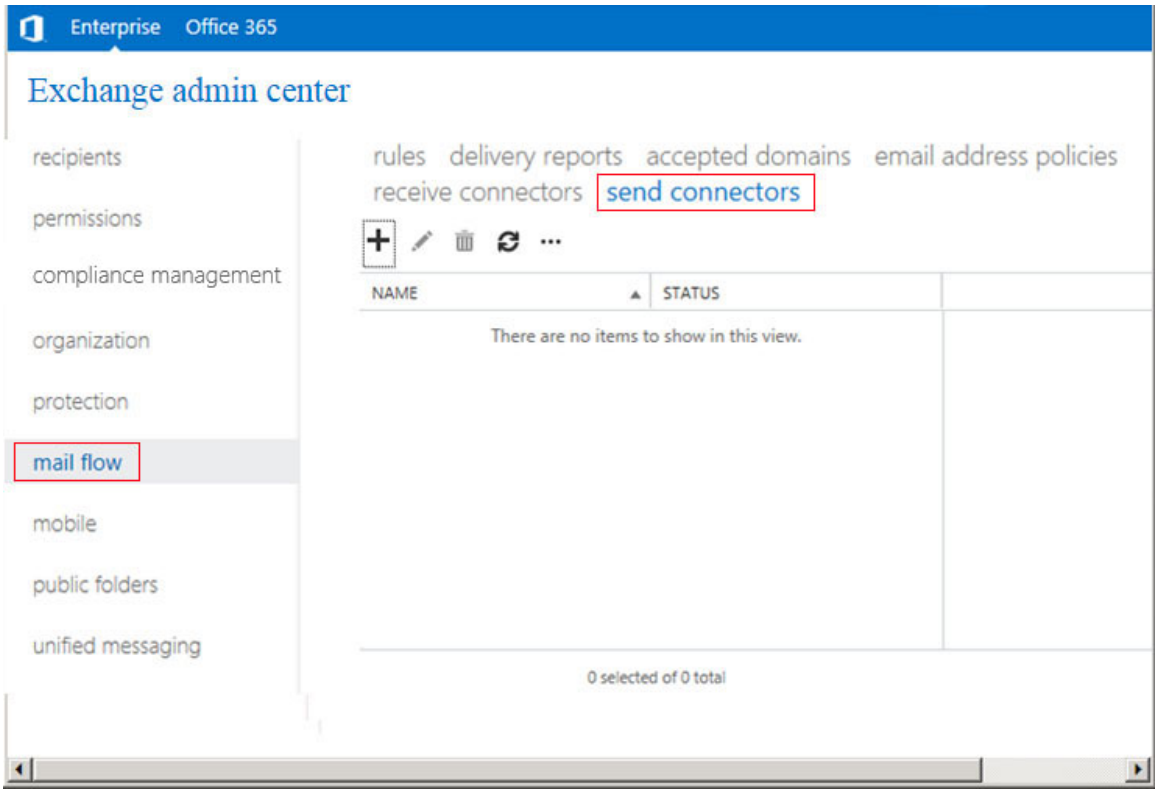
Barracuda Networks recommends hiding the alternate mail contact from the GAL; to do so, with the new mailbox still selected, click the **Edit** ( ) icon. In the **general** page, turn on **Hide from address lists**:



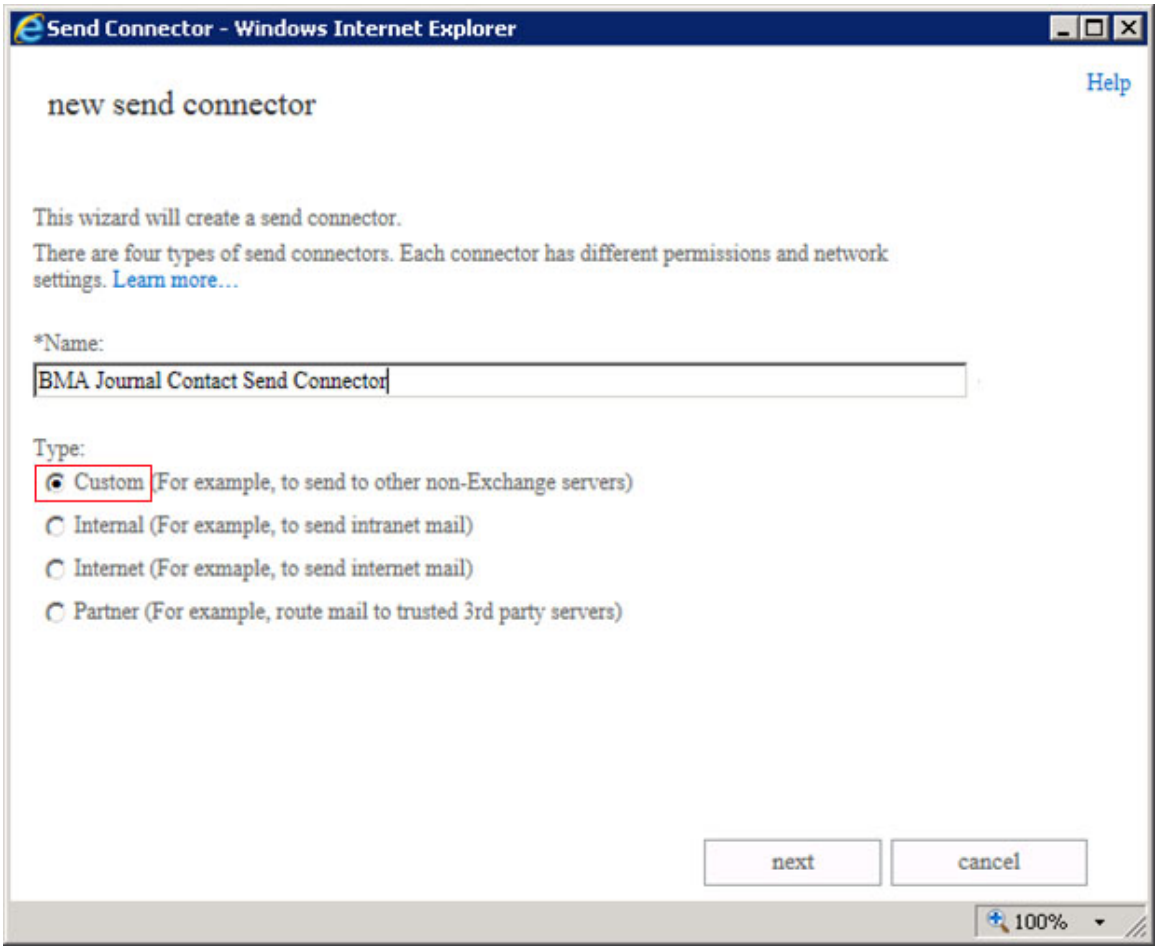
Step 4. Create a Send Connector for the Remote Domain

To route journaled mail that is sent to the contact to the Barracuda Message Archiver, use the following steps to create a Send Connector for the Remote Domain:

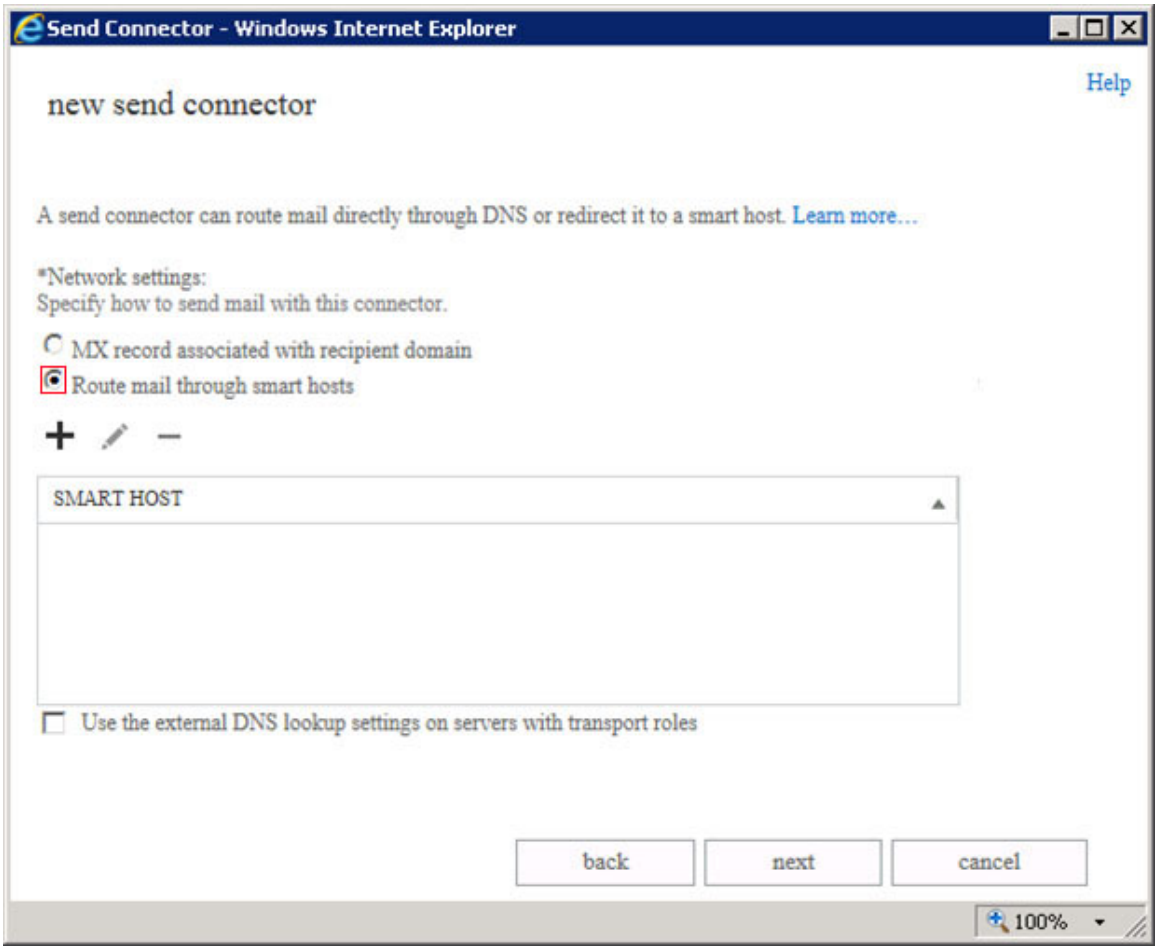
4a. Open Exchange Server 2013, and in the EAC click **mail flow** in the left pane, select **send connectors** at the top of the page, and then click the **Add** (+) icon to create a new send connector:



4b. In the **Name** field, enter a name for the connector, and in the **Type** section, select **Custom**:

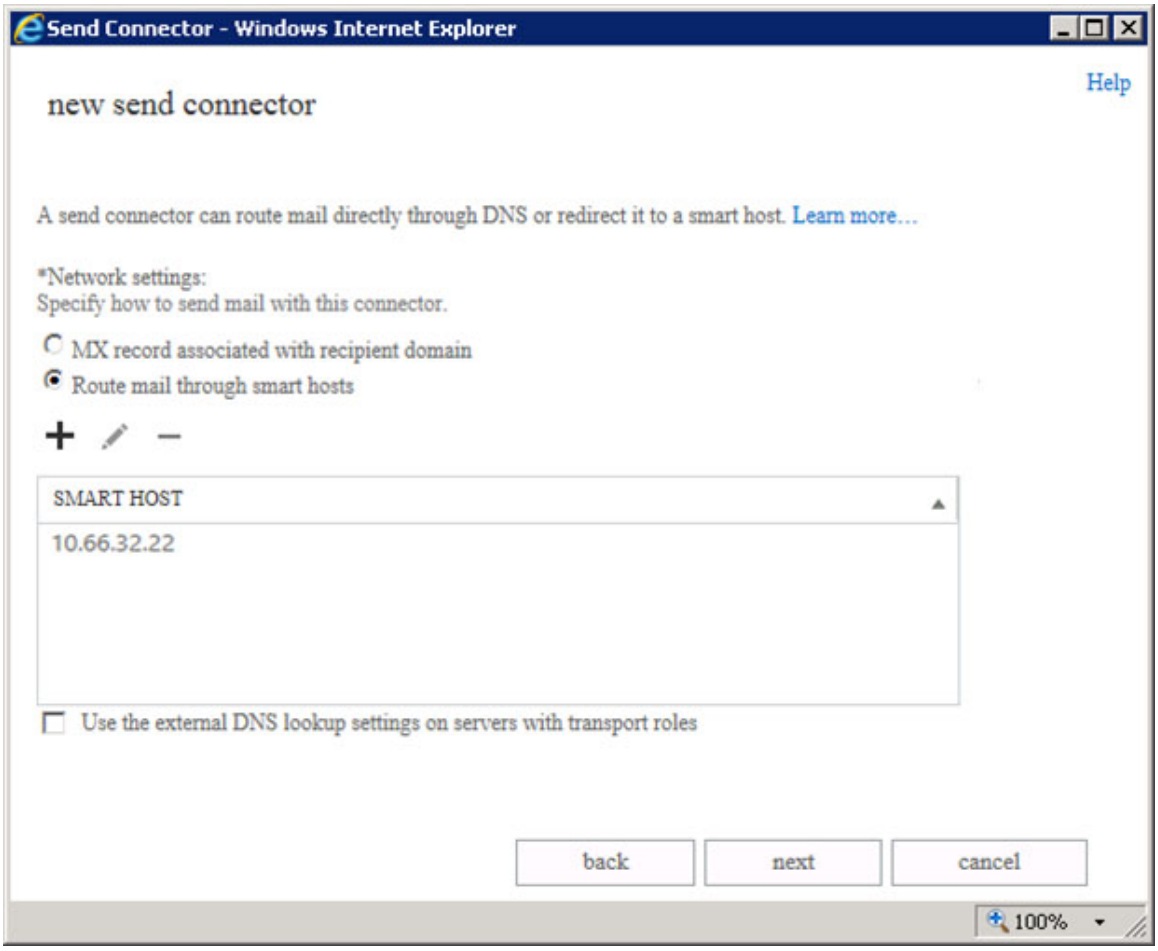

Send Connector - Windows Internet Explorer
Help
new send connector
This wizard will create a send connector.
There are four types of send connectors. Each connector has different permissions and network settings. Learn more...
*Name:
BMA Journal Contact Send Connector
Type:
Custom (For example, to send to other non-Exchange servers)
Internal (For example, to send intranet mail)
Internet (For exmaple, to send internet mail)
Partner (For example, route mail to trusted 3rd party servers)
next
cancel
100%

4c. Click **next**. In the **Network settings** page, select **Route mail through smart hosts**:

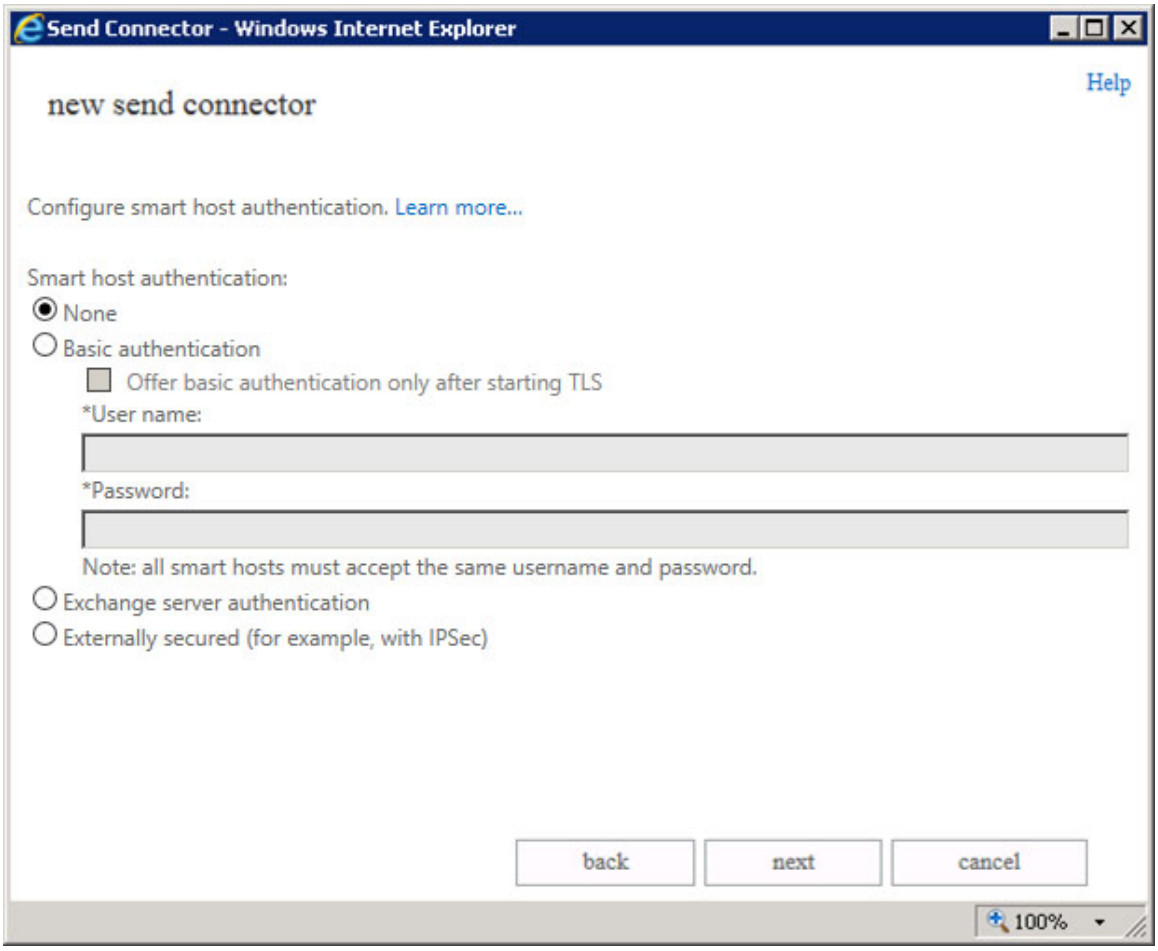

Send Connector - Windows Internet Explorer
Help
new send connector
A send connector can route mail directly through DNS or redirect it to a smart host. Learn more...
*Network settings:
Specify how to send mail with this connector.
MX record associated with recipient domain
Route mail through smart hosts
SMART HOST
Use the external DNS lookup settings on servers with transport roles
back
next
cancel
100%

4d. Click **next**. In the **add smart host** page, enter the fully qualified domain name (FQDN) or IP Address of the Barracuda Message Archiver:

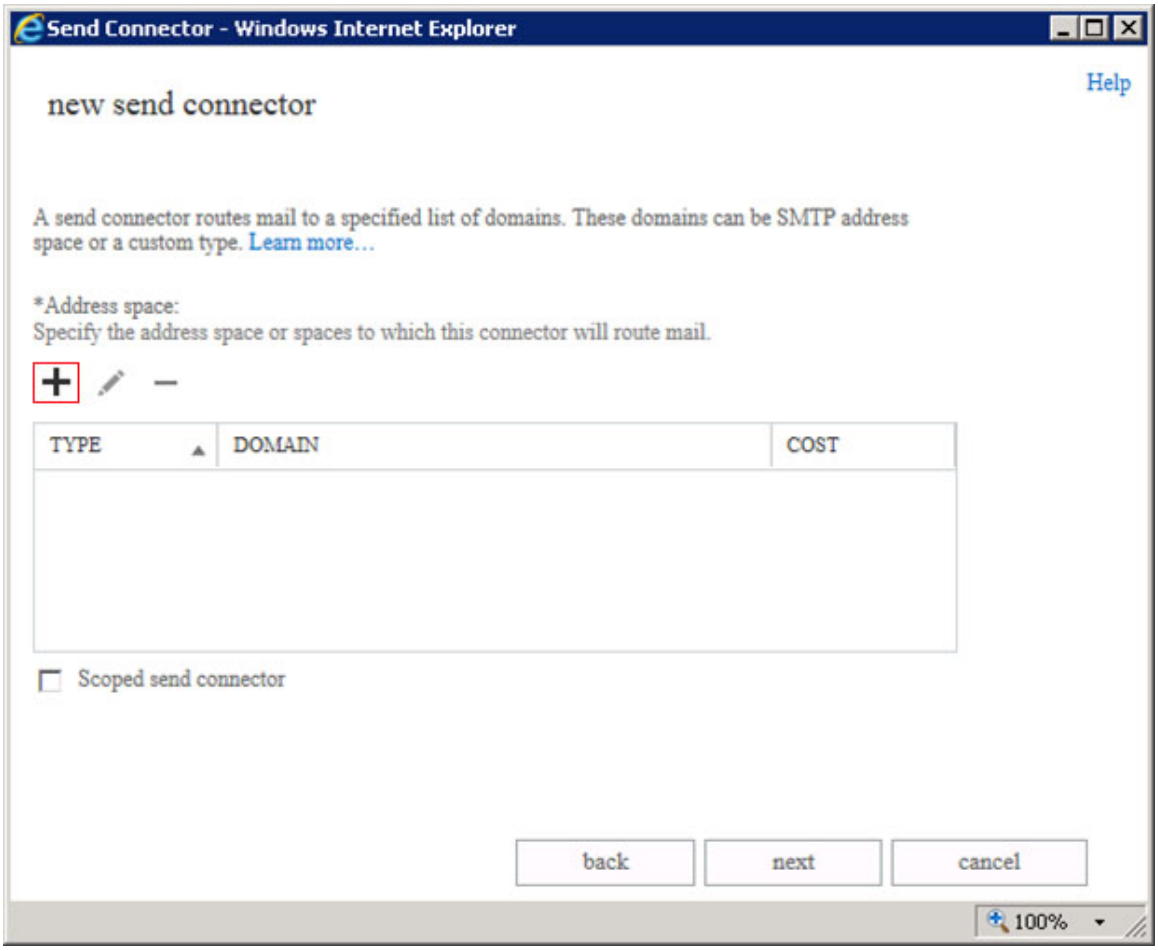
4e. Click **save**. The FQDN or IP Address displays in the **SMART HOST** list; verify the address:


Send Connector - Windows Internet Explorer
Help
new send connector
A send connector can route mail directly through DNS or redirect it to a smart host. Learn more...
*Network settings:
Specify how to send mail with this connector.
MX record associated with recipient domain
Route mail through smart hosts
SMART HOST
10.66.32.22
Use the external DNS lookup settings on servers with transport roles
back
next
cancel
100%

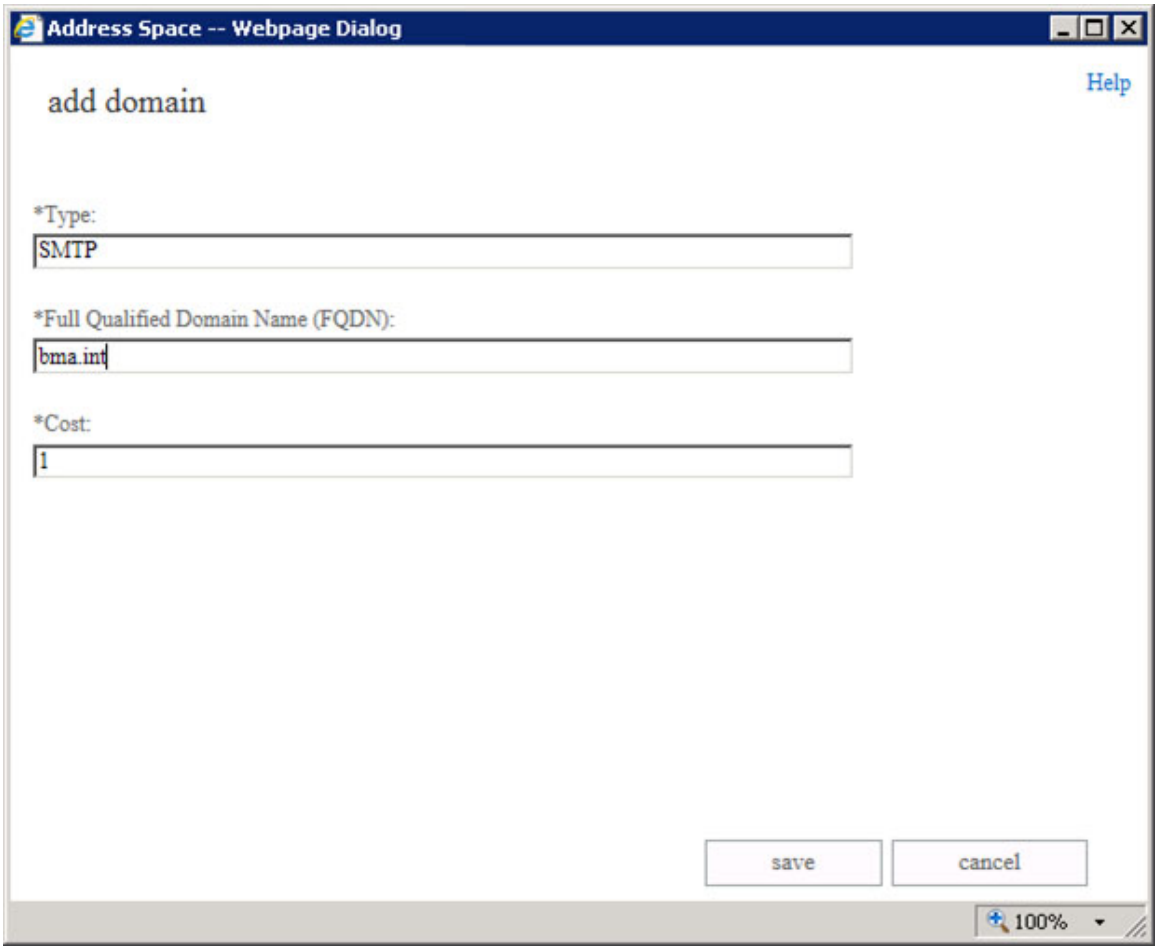
4f. Click **next**. In the **Smart host authentication** page, because authentication is not used on the smart host connection to the Barracuda Message Archiver, no changes are necessary; click **next**:



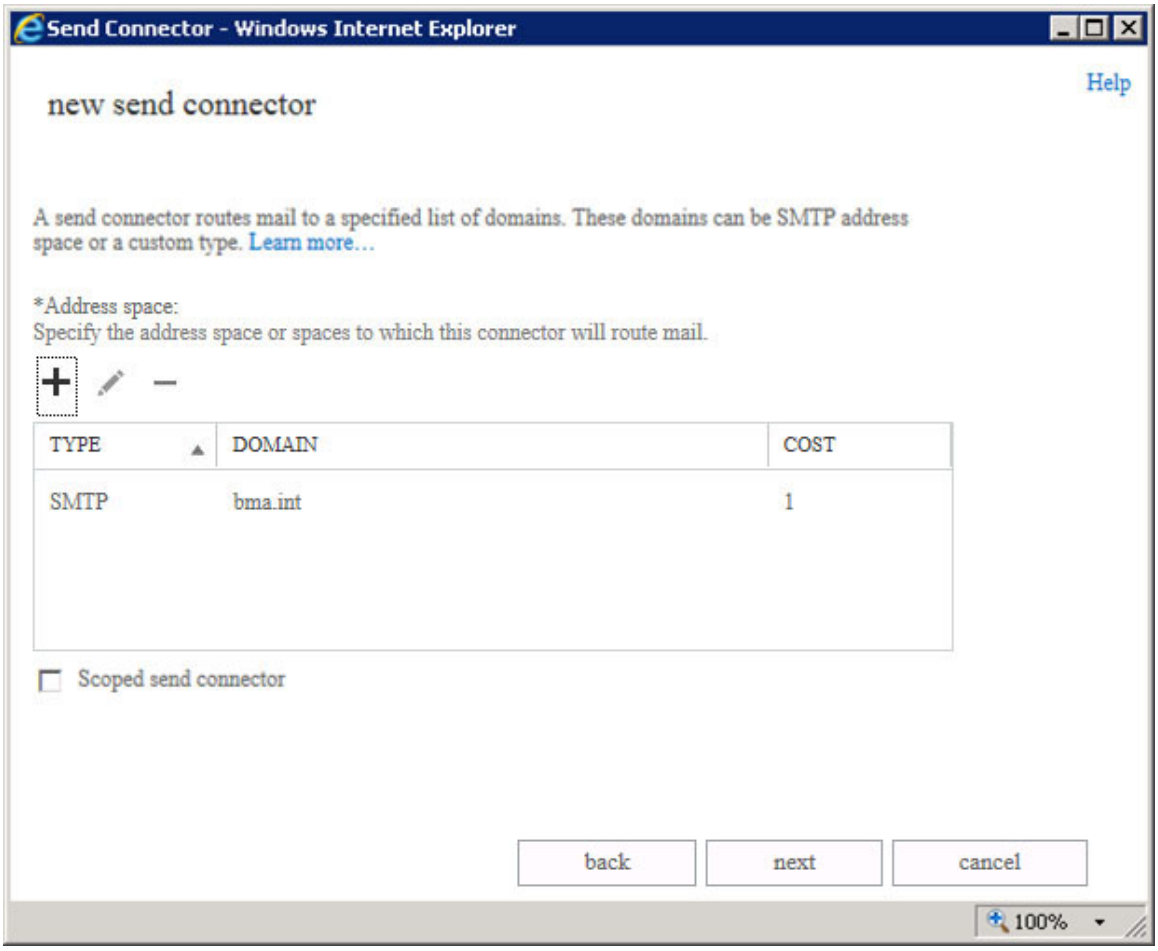
4g. In the **Address space** section, click the **Add** (+) icon:


Send Connector - Windows Internet Explorer
Help
new send connector
A send connector routes mail to a specified list of domains. These domains can be SMTP address space or a custom type. Learn more...
*Address space:
Specify the address space or spaces to which this connector will route mail.
TYPE
DOMAIN
COST
Scoped send connector
back
next
cancel
100%

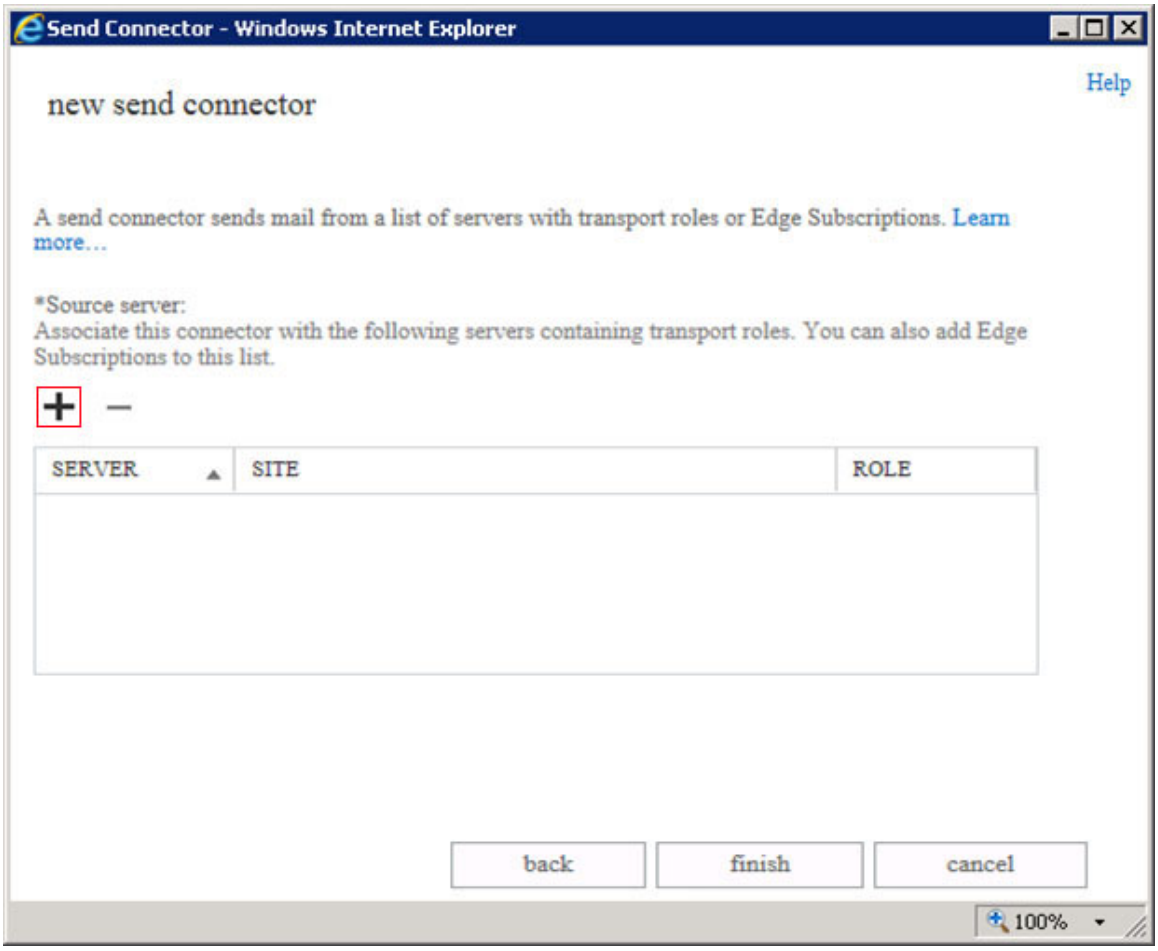
4h. In the **Address Space** page, enter the domain that matches the domain for the external email address used to create the journal contact, for example, `bma.int` (see **Step 2**):



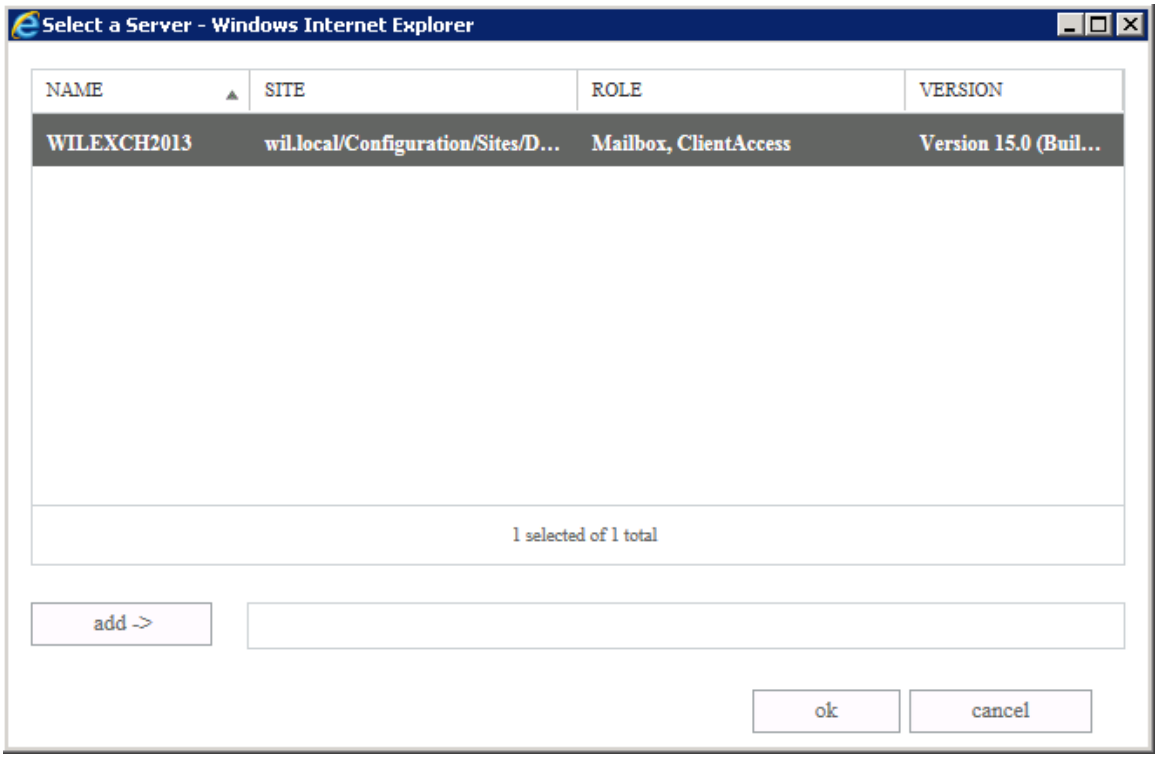
4i. The domain is added to the **Address space** list:



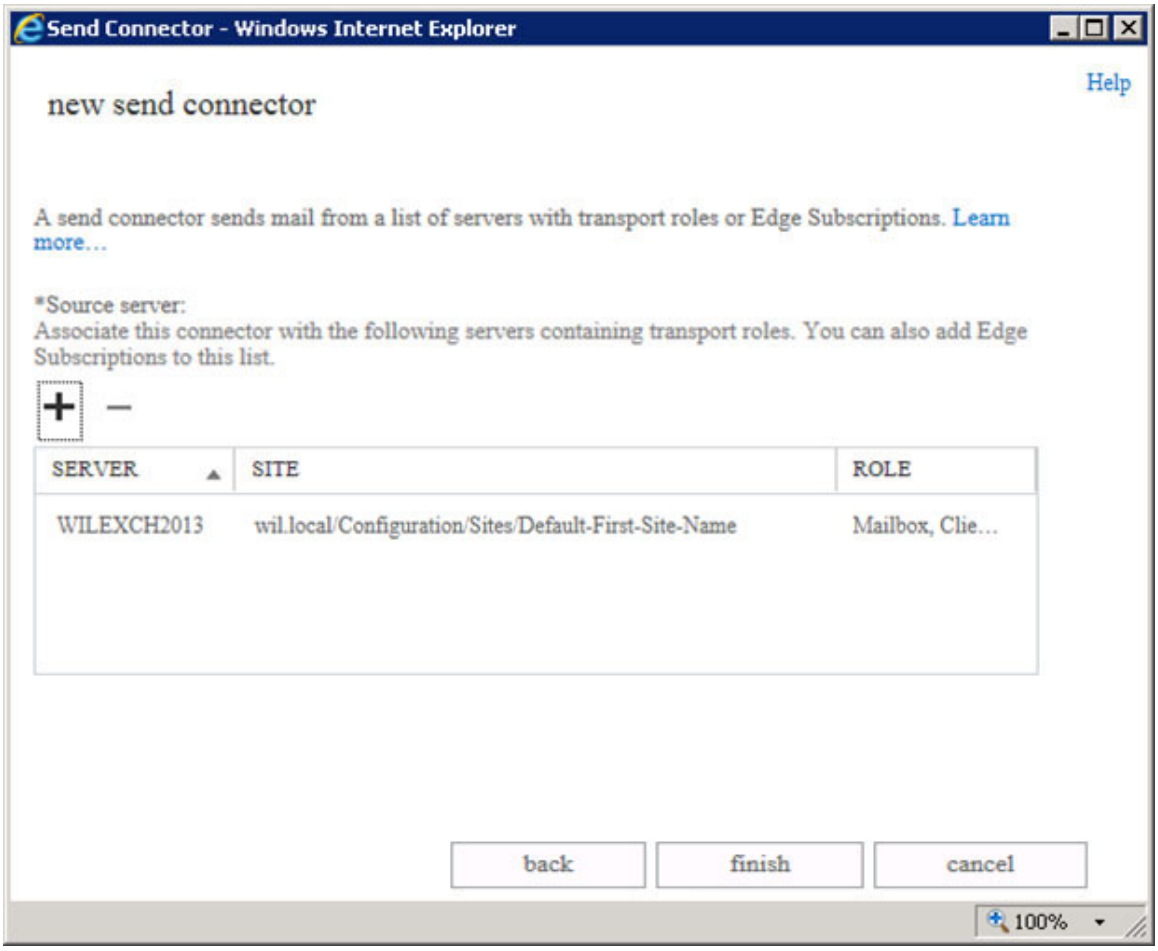
4j. Click **next**. In the **Source server** section, click the **Add** (+) icon:


Send Connector - Windows Internet Explorer
new send connector
Help
A send connector sends mail from a list of servers with transport roles or Edge Subscriptions. Learn more...
*Source server:
Associate this connector with the following servers containing transport roles. You can also add Edge Subscriptions to this list.
SERVER
SITE
ROLE
back
finish
cancel
100%

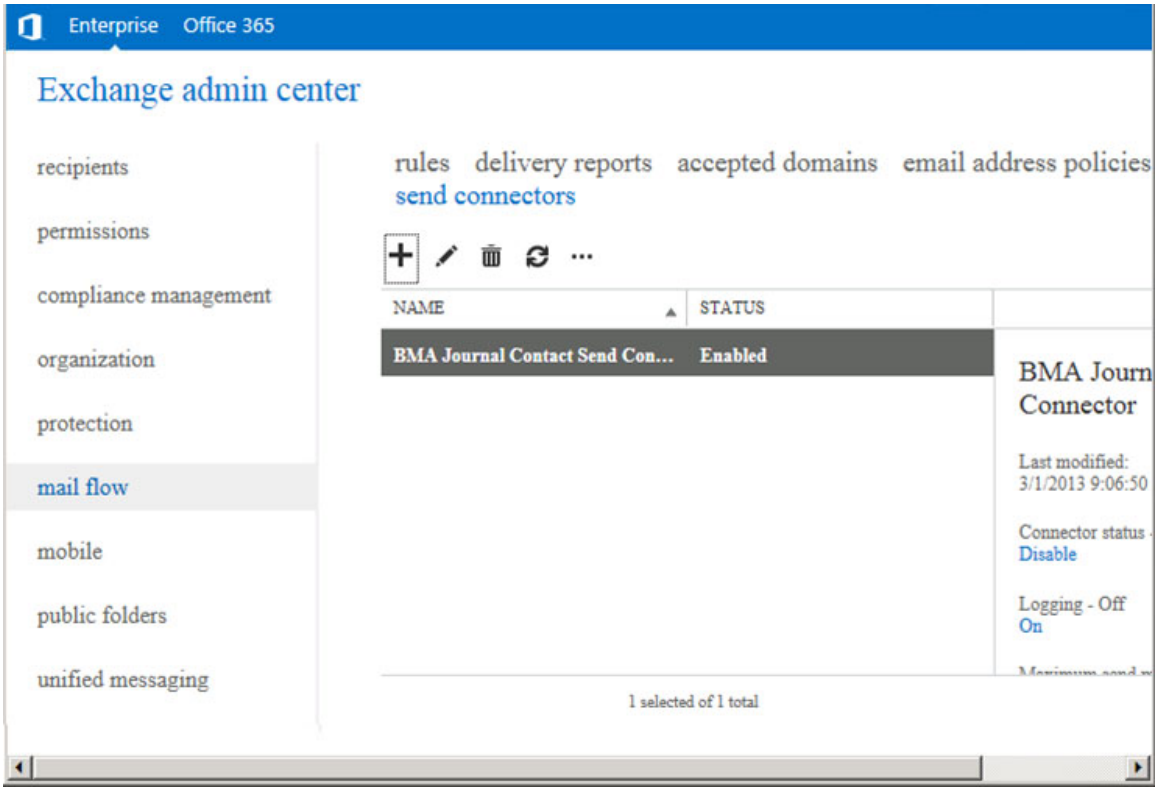
4k. Verify all of the Exchange Servers that are in the CAS role are listed; click **add** to add additional servers:



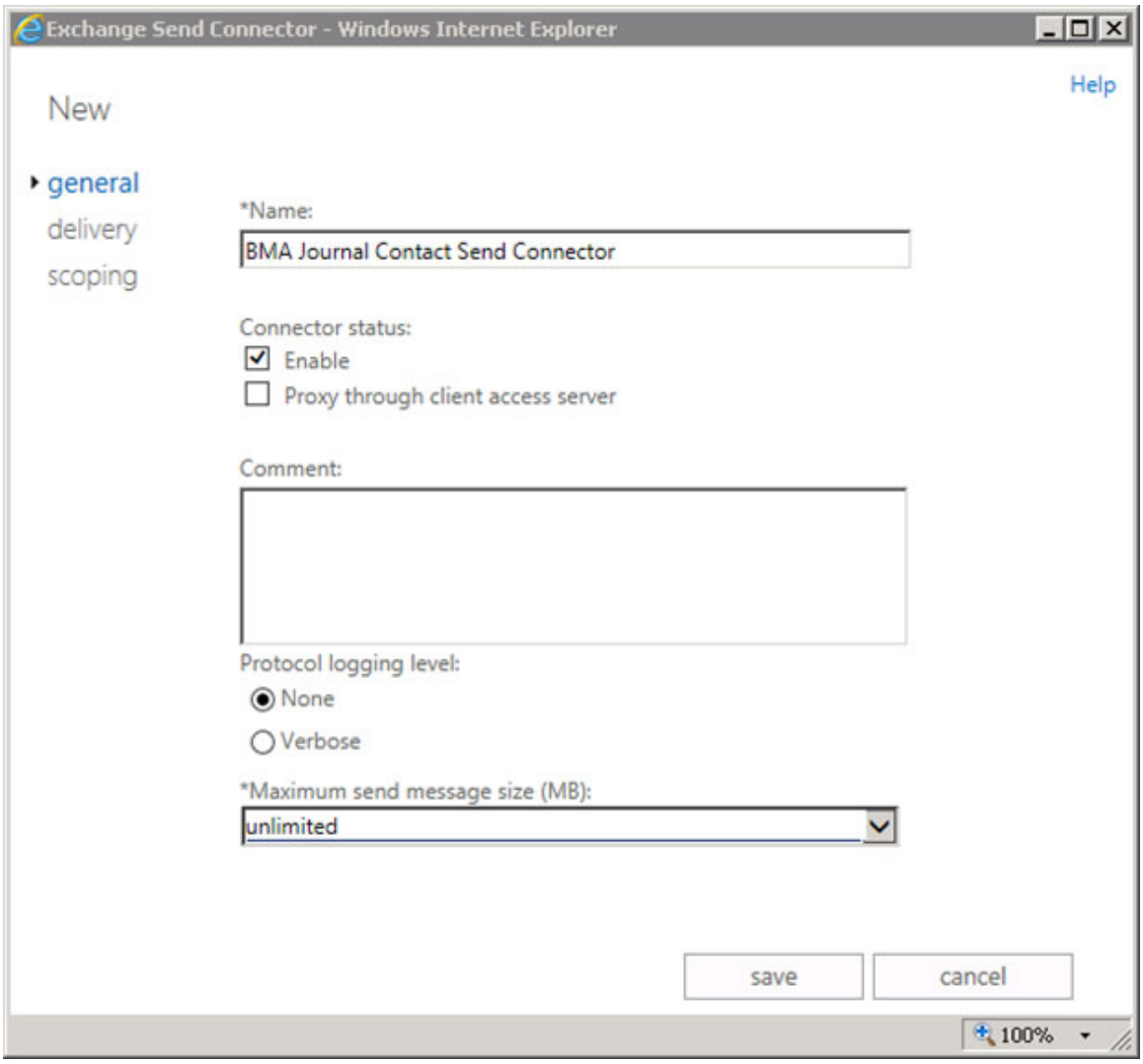
4l. Click **ok**. In the **Source server** page, the selected servers display:



4m. Click **finish**. The new send connector displays as **enabled** in the **send connectors** list:



4n. Click the Edit ( ) icon to edit the **Send Connector** properties. From the **Maximum send message size (MB)** drop-down list, select **unlimited**:



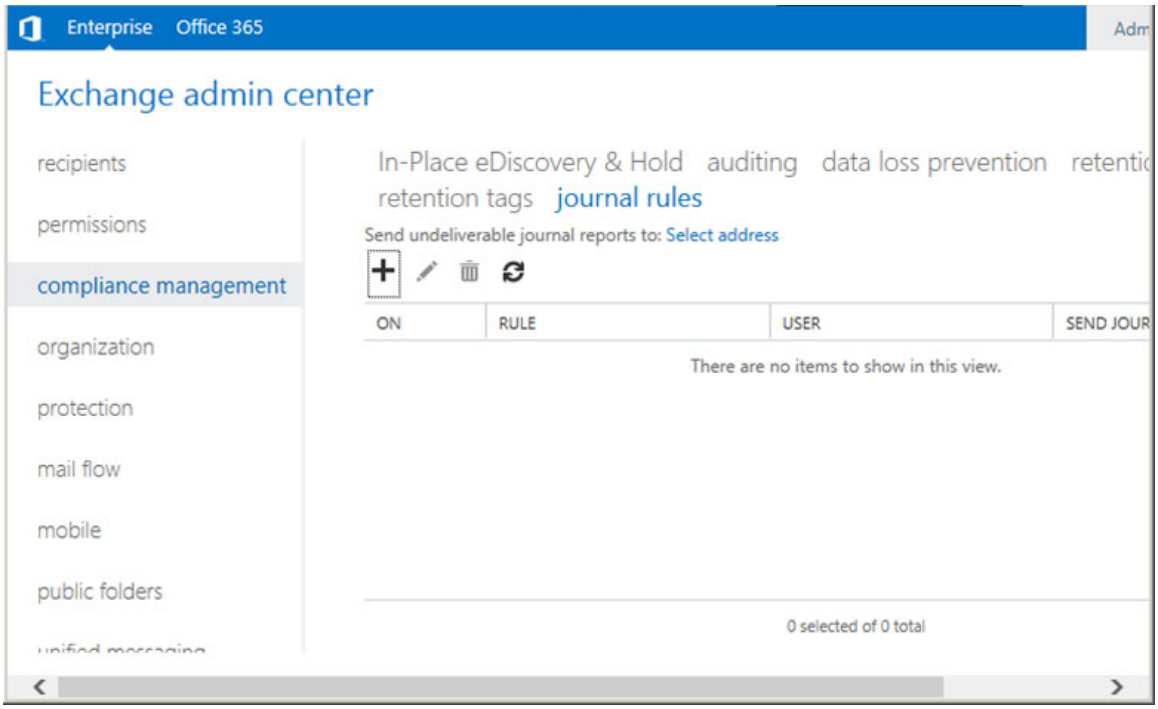
4o. Click **save**.

Step 5. Create a Journal Rule

> **Journaling**
> This article assumes you are setting up a journal rule. If you are setting up mailbox database journaling, refer to the article How to Configure Envelope (SMTP) Journaling for Microsoft Exchange Server 2013 - Standard Journaling. Use only *one* journaling method; choose the appropriate method for your environment.

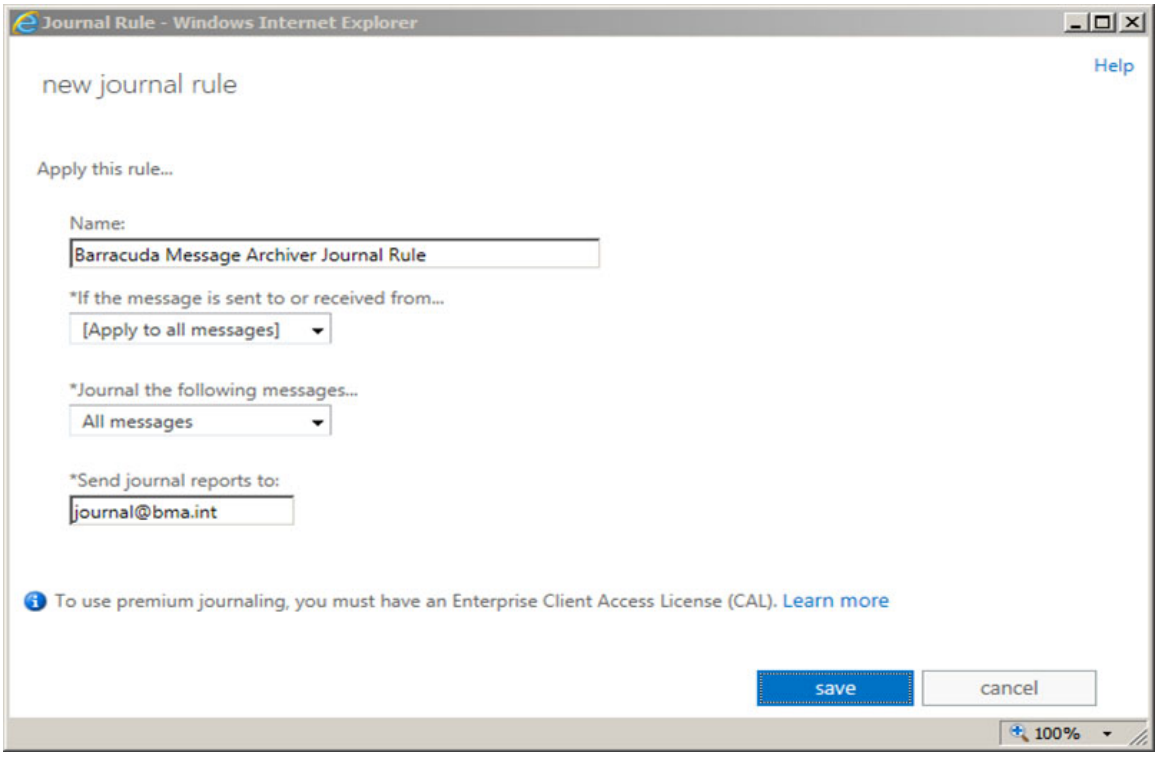
Use the following steps to set up a journal rule:

5a. Open Exchange Server 2013, and in the EAC click **compliance management** in the left pane, select **journal rules** at the top of the page, and then click the **Add** (+) icon:

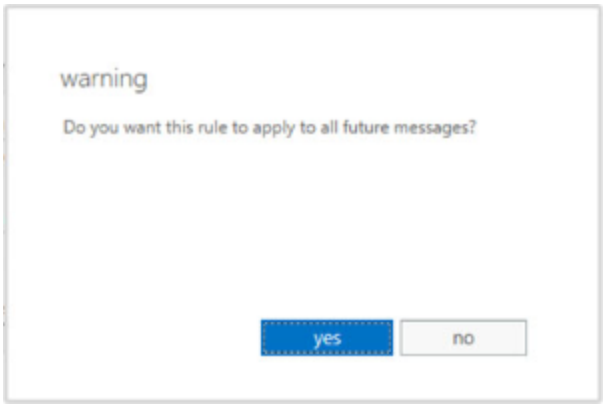


5b. In the **new journal rule** page, enter the following details:

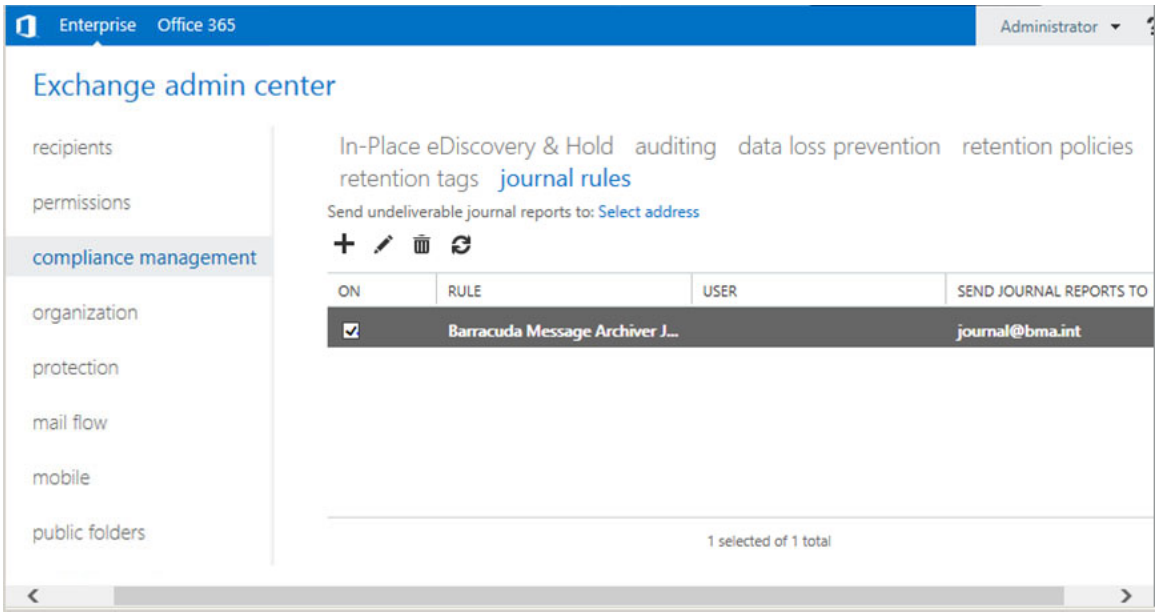
- Enter a name for the journal rule
- From the **If the message is sent or received from** list, select **Apply to all messages**
- From the **Journal the following messages** list, select **All messages**
- In the **Send Journal Reports** field, enter the email address of the contact created in **Step 4** (**bma.int**):



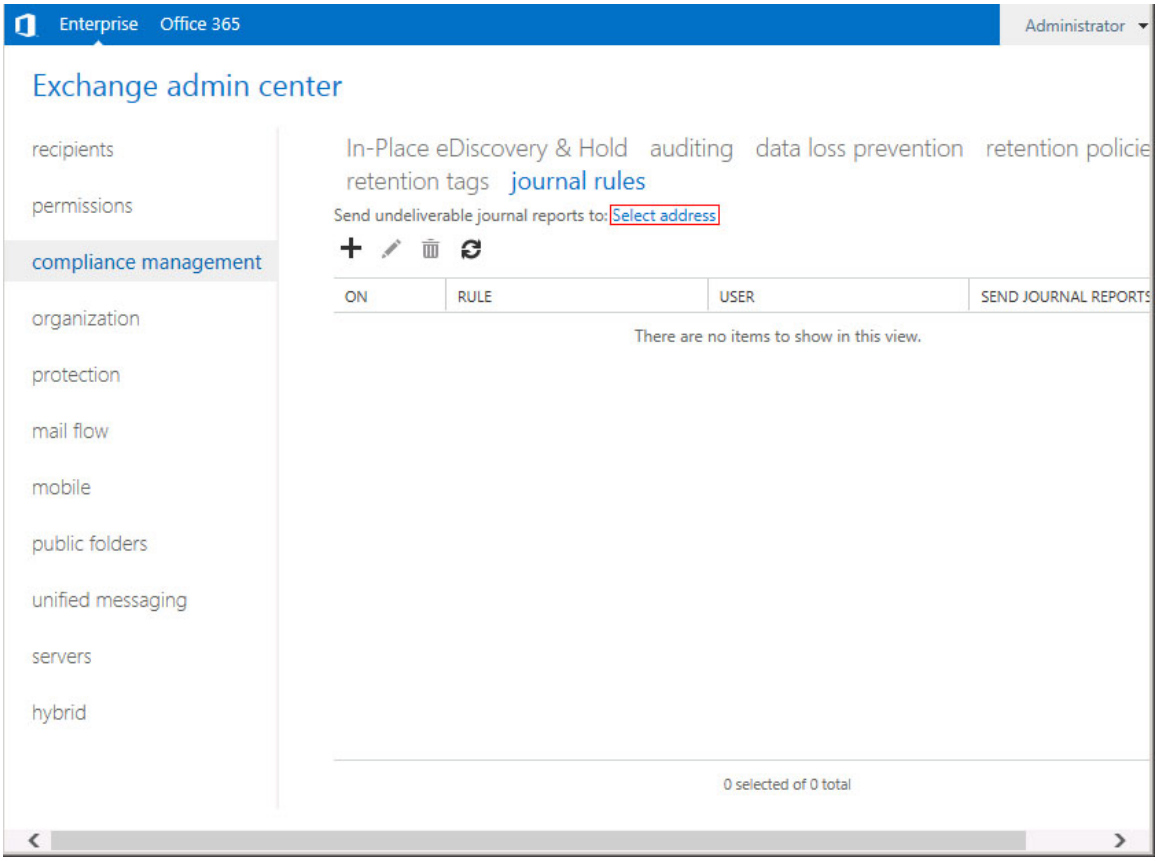
5c. Click **save**. If the warning message **Do you want this rule to apply to all future messages** displays, click **yes**:



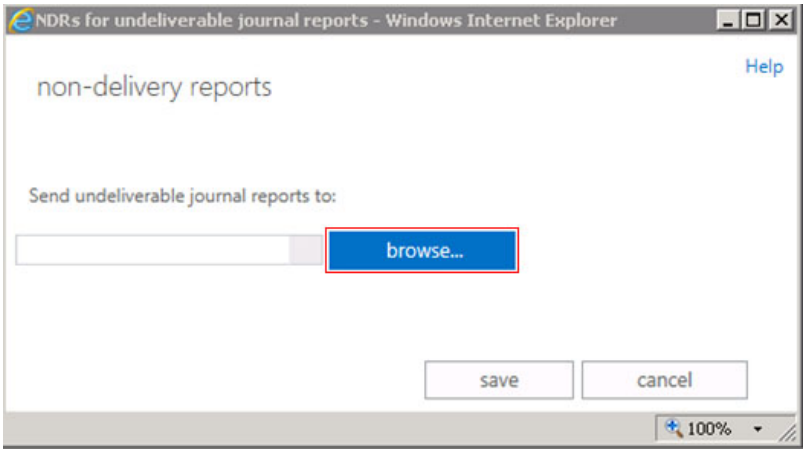
5d. The journal rule check box displays selected in the **journal rules** page:



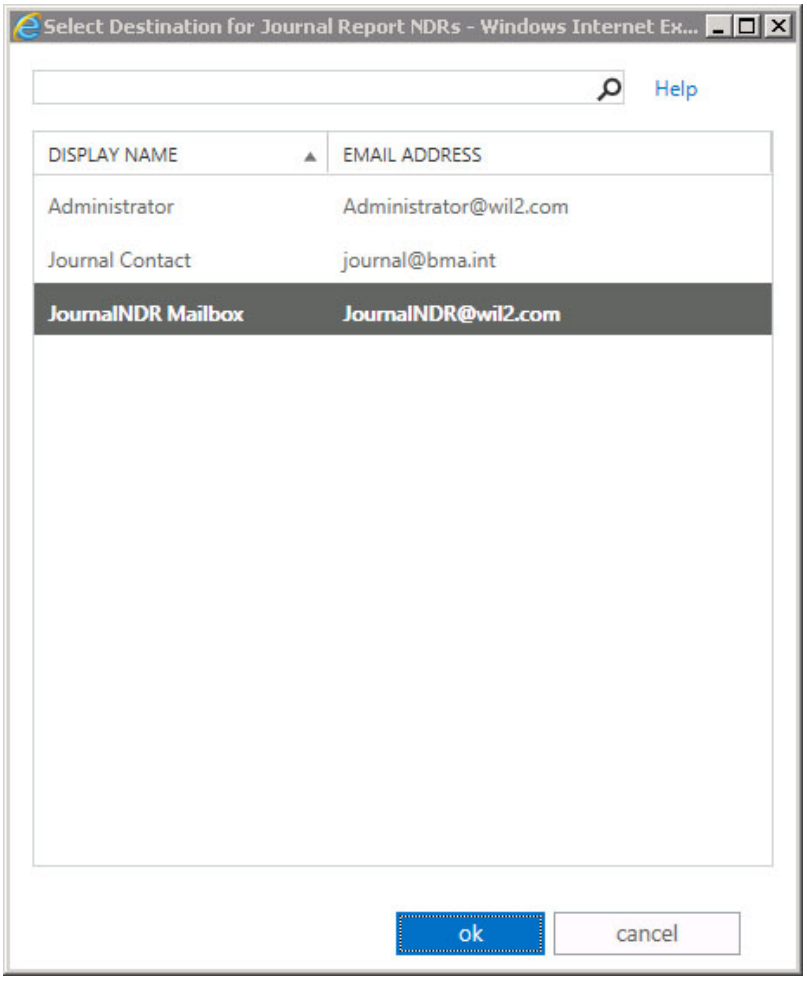
5f. In the **Send undeliverable journal reports to** section, click **Select address**:



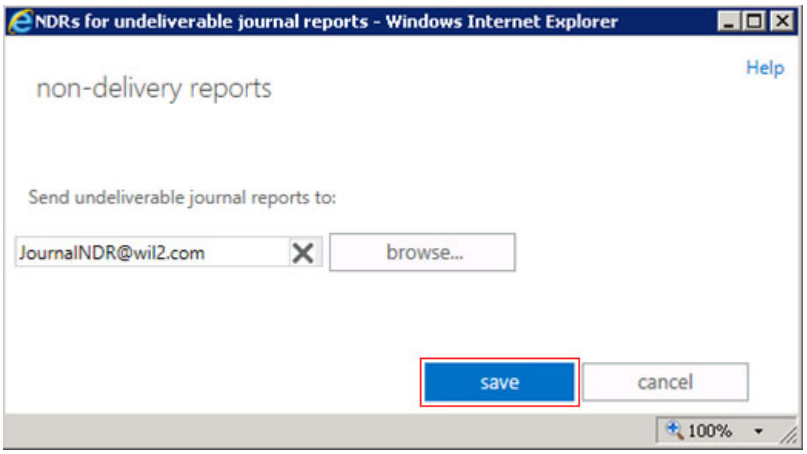
5g. In the **non-delivery reports** window, click **browse**:



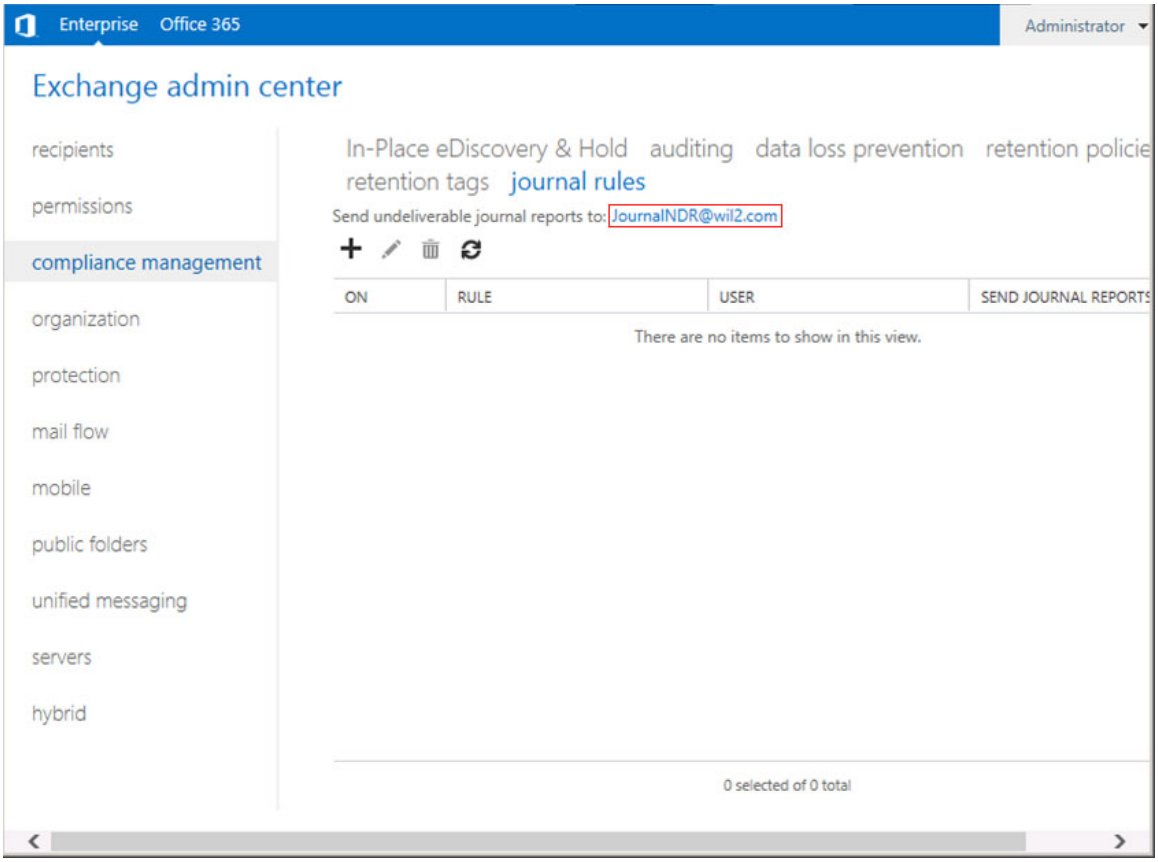
5h. Browse to and select the alternate mailbox created in **Step 3** (**Journal NDR Mailbox**):



5i. Click **ok**. Verify your selection, and then click **save**:



5j. The address displays in the **Send undeliverable journal reports to** section:



The configuration is now complete and journaled mail is forwarded to the Barracuda Message Archiver. Log into the Barracuda Message Archiver, and go to the **BASIC > Search** page in the web interface to verify that new mail is being processed. Note that it may take up to 30 minutes before journaled mail is available in the search results.

How to Configure an IMAP or POP3 Journal Account for Microsoft Exchange Server 2013

This article refers to the Barracuda Message Archiver firmware version 3.2 and higher, and a Microsoft® Exchange Server 2013.

Barracuda Networks recommends deploying your Barracuda Message Archiver with Microsoft Exchange Server 2013 using the push method, alternately, you can set up IMAP or POP3 journal accounts as described in this article.

You can configure the Barracuda Message Archiver to automatically retrieve messages directly from your mail server using the IMAP4 or POP3 protocol.

In this article:

- Setting Up a POP3 Journal Account
  - Step 1. Enable POP3
  - Step 2. Start the POP3 Services
- Setting Up an IMAP Journal Account
- Add a Journal Account to the Barracuda Message Archiver

Related Articles

- Understanding Microsoft Exchange 2013 Journaling

Additional Resources
• Microsoft Exchange Permissions Depending on your deployment, refer to Microsoft TechNet for configuration requirements: • Enable POP3 in Exchange 2013 • Enable IMAP4 in Exchange 2013

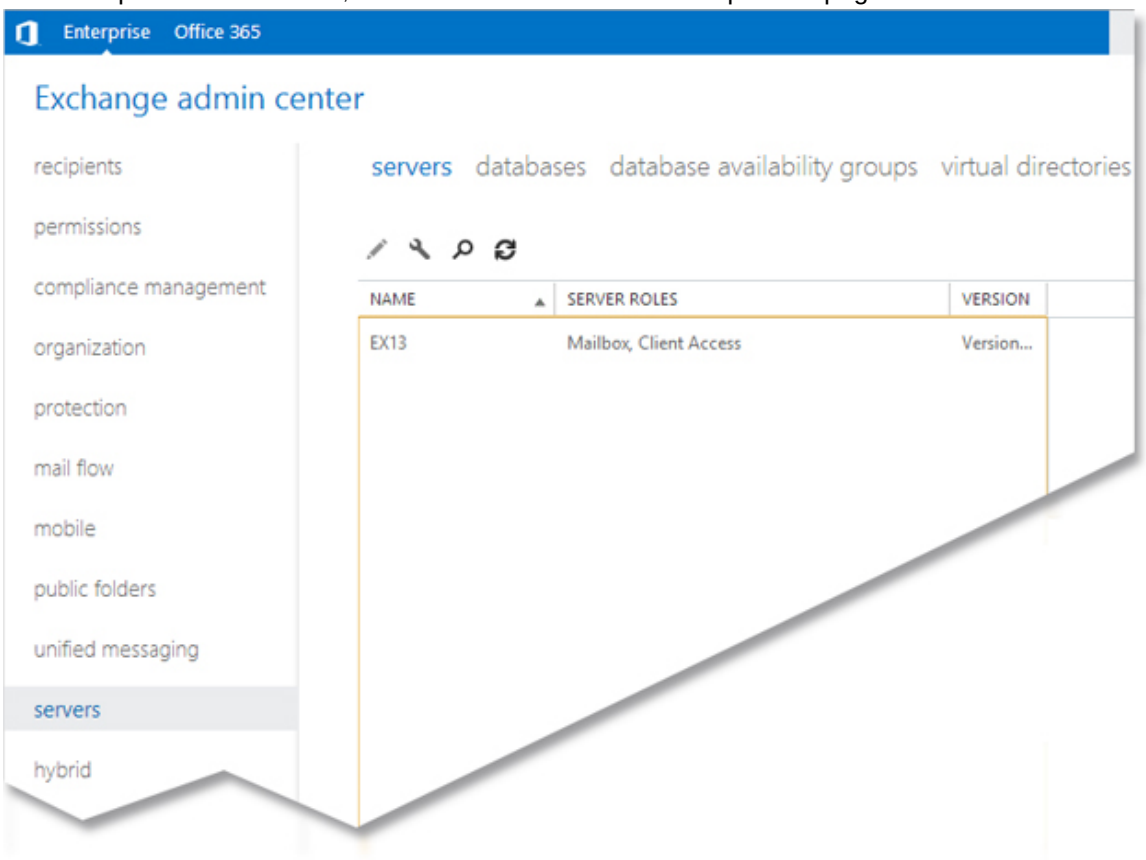
⚠ The maximum size email that will be retrieved by the Barracuda Message Archiver via POP or IMAP is 100MB.

Setting Up a POP3 Journal Account

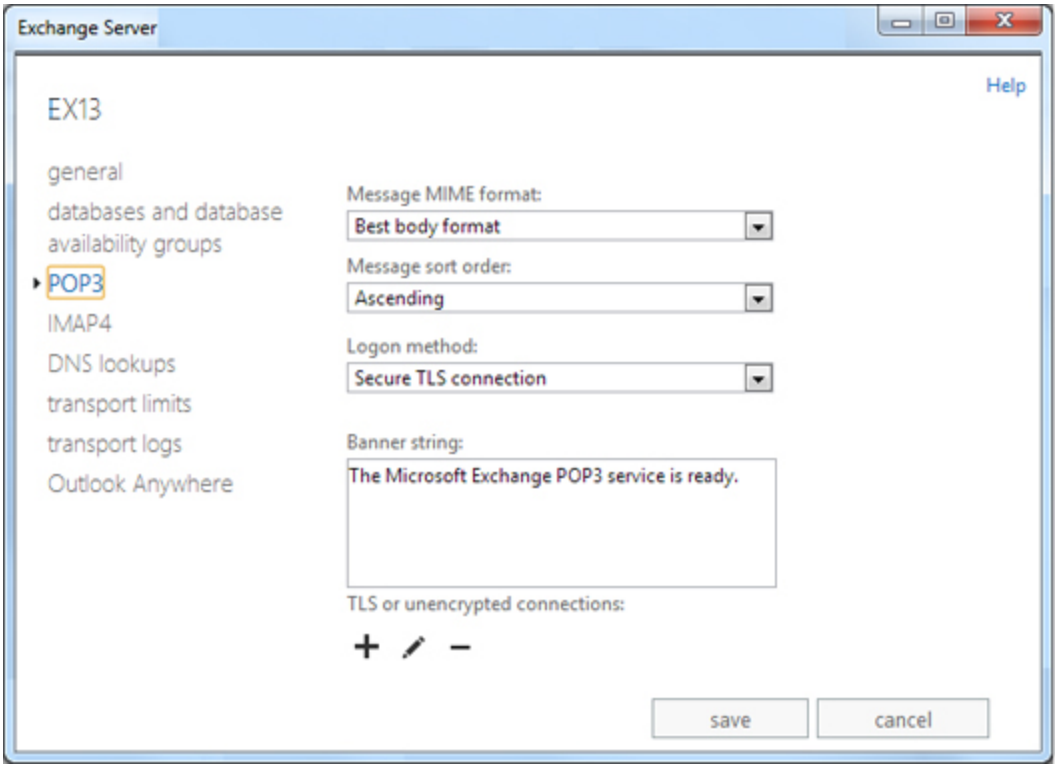
Step 1. Enable POP3

Use the following steps to enable POP3 on your Exchange 2013 Server.

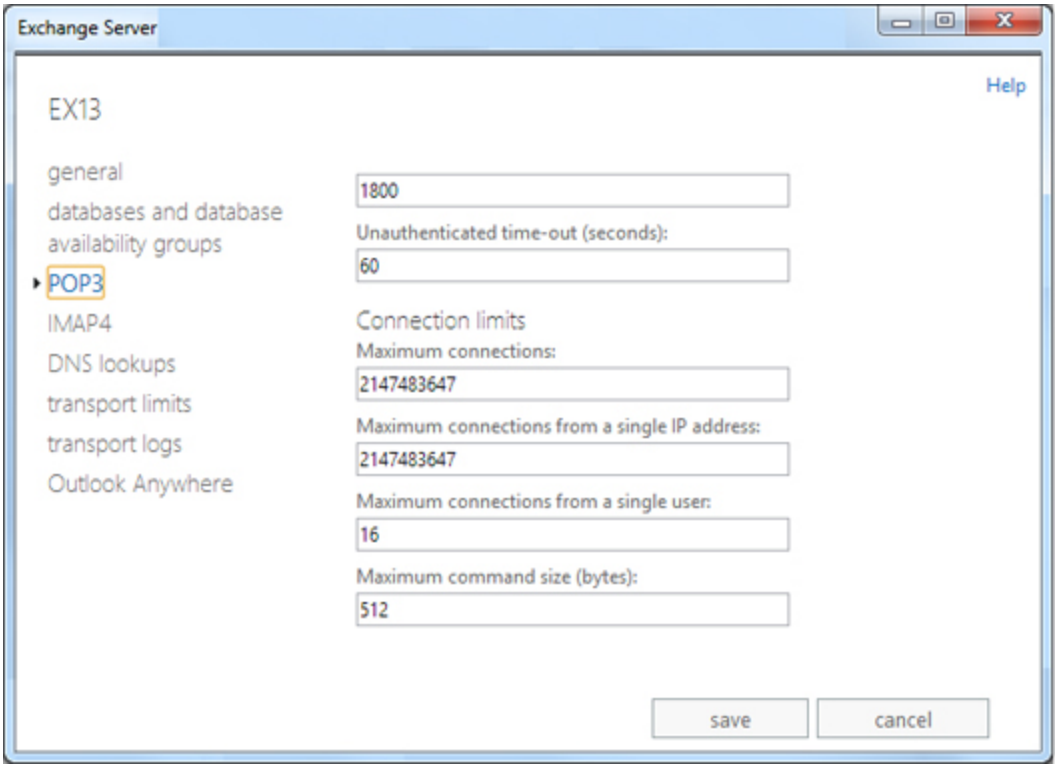
1. Log in to the Exchange Server as the Exchange Server Administrator, and navigate to the Exchange admin center (EAC): `https://<Exchange_server_name>/ecp`
2. In the left pane click **Servers**, and then click **Servers** at the top of the page:



3. Select the Client Access server, and then click **Edit (**).
4. On the server properties page, click **POP3**:



5. Scroll down and click **More options**.
6. Under **Connection limits**, use the following settings:
    - In the **Maximum connections** field, specify the total number of authenticated and unauthenticated connections the specified server can accept. The default value is 2,147,483,647; enter a value between 1 and 2,147,483,647.
    - In the **Maximum connections from a single IP address** field, specify the number of connections that the server can accept from a single IP address. The default value is 2,147,483,647; enter a value between 1 and 2,147,483,647.
    - In the **Maximum connections from a single user** field, specify the maximum number of connections that the server can accept from a particular user. The default value is 16. Enter a value between 1 and 16.
    - In the **Maximum command size (bytes)** field, specify the maximum size of a single command. The default size is 512. Enter a value between 40 and 1,024.



7. Click **save**, and then click **ok** in the warning dialog to save your changes.

Step 2. Start the POP3 Services

Use the following steps to start the POP3 services; you must log in as the system administrator to complete these steps:

1. Log into the system running the Client Access server role, and open **Services** (**Start > Programs** > **Administrative Tools** > **Services**). Right-click **Microsoft Exchange POP3**, and then click **Start**.
2. Log into the system running the Mailbox server role, and open **Services** (**Start** >**Programs** > **Administrative Tools > Services**). Right-click **Microsoft Exchange POP3 Backend**, and then click **Start**.

Setting Up an IMAP Journal Account

By default, IMAP4 client connectivity is not enabled on Microsoft Exchange Server 2013. To enable IMAP4 client connectivity, you must start both of the following IMAP services:

- Microsoft Exchange IMAP4 Service
- Microsoft Exchange IMAP4 Backend Service

Once enabled, Exchange 2013 accepts unsecured IMAP4 client communications on port 143, and over port 993 using Secure Sockets Layer (SSL).

For configuration and testing details, refer to the following sections in the Microsoft TechNet article Enable IMAP4 in Exchange 2013:

- *Use the Microsoft Management Console Services snap-in to enable IMAP4*
- *Use the Shell to enable IMAP4*
- *How do you know this worked?*

Add a Journal Account to the Barracuda Message Archiver

Once you configure the Service on your Exchange Server, you can add the journal account to the Barracuda Message Archiver to begin retrieving new messages for archiving.

1. Log in to the Barracuda Message Archiver as the administrator, and go to **MAIL SOURCES > Journal Accounts**.
2. In the **Journal Accounts** section, enter the following details:
    - **Enable Journal Accounts** – Select **Yes** to allow the Barracuda Message Archiver to poll the listed accounts for new messages for archiving.
    - **Enable Journal** – When set to **Yes**, all listed accounts are tested for connectivity with each page view**.**
    - **Polling Frequency** – Specify how often to poll each journal account for new messages

3. In the **Journal Accounts Configuration** section, specify the following details for each journal account:
    - **Status** – Displays the connection status for each account.
    - **Server** – Enter the hostname of the mail server where the account resides.
    - **Protocol** – Select whether the account is POP3 or IMAP; once you select the protocol, the default port number automatically populates the **Port** field.
    - **Username** – Enter the username or ID associated with this mailbox as defined by your server. This is usually the mailbox designated as the "journaling" email address on your mail server, and specified by the complete email address such as **journal @example.com**.
    - **Password** – Enter the password associated with the username.
    - **Encryption** – Select the type of encryption used to connect to the mail server:
        - **TLS (if available)**
        - **TLS**
        - **SSL**
        - **None**
    - **Port** – Select the associated port based on the selected protocol; the default value is port 143 for **IMAP**, and port 110 for **POP3**.
4. **Keep Items on Server**:
    - Select **Off** to allow the Barracuda Message Archiver to automatically clean up the content of the journal mailbox after each import.
    - Select **On** to prevent the Barracuda Message Archiver from removing the journaled messages from the mail server; *only* turn this option on if the contents of the journal account is required by other applications. In this case, make sure that another method for cleaning up the journal account is enabled on the mail server in order to prevent unlimited growth on the mail server and to stay in compliance with your organization's message retention policies.

    > Barracuda Networks recommends that you deselect **Keep Items on Server** to save hard drive space on your mail server.

5. Click **Add** to add the journal account; verify the **Status** field displays green, and then click **Save Changes**.
6. To remove a journal account, click the **Delete** ( ) icon, and confirm you want to remove the account.

How to Disable Throttling in Microsoft Exchange Server 2013

> This article refers to the Barracuda Message Archiver release 3.5 or higher, and Microsoft® Exchange Server 2013. If you are using Microsoft Exchange Server 2010, refer to How to Disable Throttling in Microsoft Exchange Server 2007 and 2010.

Microsoft Exchange Server 2013 message throttling policies set bandwidth limits and restrict the number of processed messages. Throttling is enabled by default on Microsoft Exchange 2013. In order to disable throttling, you must create an appropriate policy and assign it to the service account as documented in the Microsoft Technet article Set Throttling Policy.

> Following is a guideline; adjust as necessary for your environment.

Create a New Account

> **Service Account**
> For more information on creating a Service account, refer to Creating an Email Service Account for Microsoft Exchange Server.

Use the following steps to create a new account:

1. Log in to the Exchange Server as the administrator, and open the **Exchange admin center**.
2. Go to **recipients > mailboxes**, and click the plus (**+**) symbol, and click **User mailbox**.
3. In the **new user mailbox** window, enter the new user details, for example, `PolicyAdmin`.
4. Click **Save**. Double-click the new user mailbox to open the **Properties**.
5. Enter the account details in the **General** tab, and then click **Apply**.
6. Click the **Member Of** tab, and add the user as a member of the **Domain Users** group.

Assign Permissions

Use the following steps to assign permissions to the account created in the previous step:

1. Log in to the Exchange Server as the administrator, and open the **Exchange Management Shell** .
2. At the command prompt, type the following command:
   `New-ManagementRoleAssignment -Name:BarracudaMessageArchiver -Role:ApplicationImpersonation -User:PolicyAdmin`
   Where *PolicyAdmin* represents the new account name.

Disable Throttling Policy Enforcement

Use the following steps to disable throttling policy enforcement on the new account, replacing *PolicyAdmin* with the new account name:

1. Log in to the Exchange Server as the administrator, and open the **Exchange Management Shell.**
2. At the command prompt, type the following command to create a new throttling policy:
   `New-ThrottlingPolicy PolicyAdminPolicy`
3. Press **Enter**. Type the following command to set the throttling policy:
   `Set-ThrottlingPolicy PolicyAdminPolicy -RCAMaxConcurrency Unlimited -EWSMaxConcurrency Unlimited -EWSMaxSubscriptions Unlimited -CPAMaxConcurrency Unlimited -EwsCutoffBalance Unlimited -EwsMaxBurst Unlimited -EwsRechargeRate Unlimited`
4. Press **Enter**. type the following command to disable policy enforcement:
   `Set-Mailbox "PolicyAdmin" -ThrottlingPolicy PolicyAdminPolicy`
5. Press **Enter**.

Microsoft Exchange Server 2007 and 2010 Deployment

Recommended Deployment Method

- Microsoft Exchange Server 2007 and 2010 Deployment Template
- Understanding Microsoft Exchange Server 2007 and 2010 Envelope Journaling
- Configuring Envelope Journaling for Microsoft Exchange Server 2007 and 2010

Alternate Method

- Configuring an IMAP or POP3 Journal Account for Microsoft Exchange Server 2007 and 2010

See Also

- Microsoft Exchange Server 2003, 2007, and 2010 Integration describes how to automatically import, stub, and synchronize Microsoft Exchange Server folder data.
- Exchange Server 2010 SP1 Shared Mailbox Support

Microsoft Exchange Server 2007 and 2010 Deployment Template

> This article refers to the Barracuda Message Archiver firmware version 3.1 and higher, and a Microsoft® Exchange Server 2007 and 2010. RPC over HTTP (RoH) is available in release 3.5 and higher.

This template is a based on a *typical onsite deployment* of the Barracuda Message Archiver with Microsoft Exchange Server 2007/2010 Standard or Enterprise version using envelope (SMTP) journaling. This template describes the initial Barracuda Message Archiver setup for this deployment.

In this article:

- Implementation Prerequisites
- Physical Installation and Console Configuration
- Firewall Ports
- Activation
- Basic and Administration Setup
- Enable SMTP Forwarding on the Barracuda Message Archiver

- Enable Journaling
- Configure Exchange Integration Operations
    - Email Service Account Creation

Related Articles

- Message Archiving Concepts
- Message Import, Stubbing & Configuration
- Search Options & Configuration

Stubbing and Microsoft Exchange Import

For stubbing and Microsoft Exchange imports initiated via the Barracuda Message Archiver web interface, there is a 100MB limit on file import.

Configuration Guidelines

This article is intended as a configuration *guideline*; your deployment will be specific to your environment. Any administrative changes should be reviewed with your IT team before proceeding.

If you are migrating to a newer version of Exchange Server, refer to the Barracuda Message Archiver and Microsoft Exchange Server Migration overview for more information.

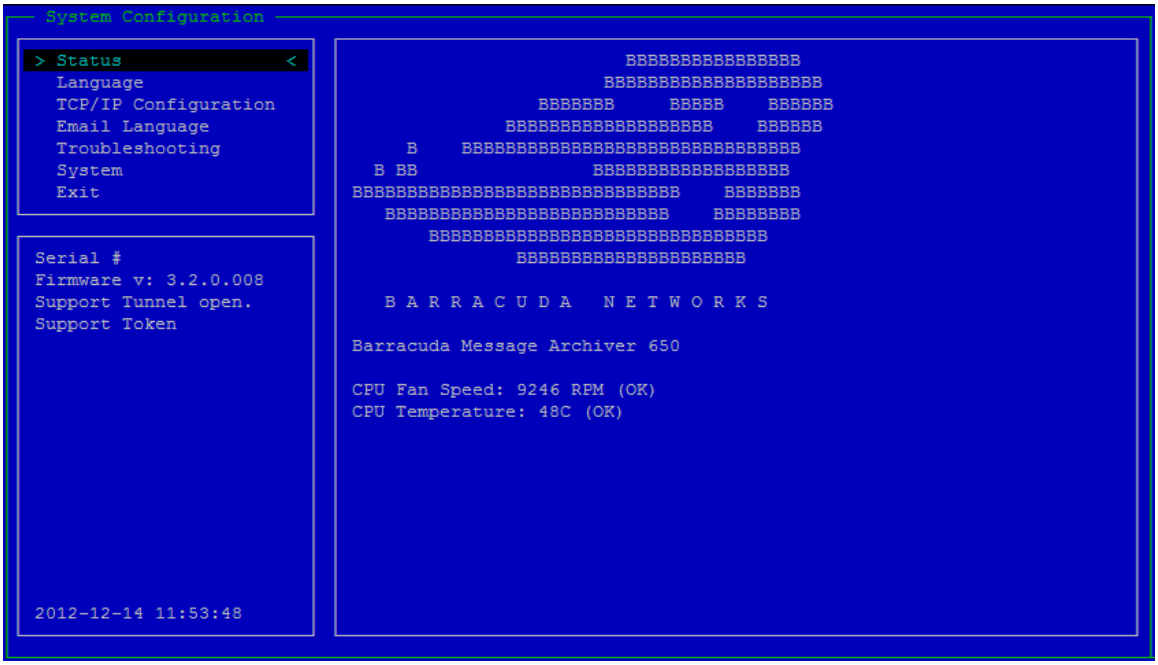
Implementation Prerequisites

You will need configuration Access to the Exchange environment, and the ability to make firewall changes, if deemed necessary.

Physical Installation and Console Configuration

Physically install the Barracuda Message Archiver using the following steps:

1. Fasten the Barracuda Message Archiver to a 19-inch rack or place it in a stable location.
2. Connect an Ethernet cable from the network switch to the Ethernet port on the back of the Barracuda Message Archiver.
3. Connect a standard VGA monitor, PS2 keyboard, and an AC power cord to the Barracuda Message Archiver. Press the **Power** button on the front panel to turn the unit on.
4. Log into the console using **admin/admin**, and configure the **IP Address, Subnet Mask, Default Gateway, Primary DNS Server**, and **Secondary DNS Server** as appropriate for your network:



Firewall Ports

If the Barracuda Message Archiver is located behind a corporate firewall, open the following ports on the firewall to ensure proper operation:

Port	Direction	TCP	UDP	Usage
22	Out	Yes	No	Remote diagnostics and service *recommended* (1)
25	Out	Yes	No	Email and bounces (25 inbound may be necessary for some deployments)
53	Out	Yes	Yes	Domain Name Service (DNS) *recommended*
80 and 443	Out	Yes	No	Virus, Policy, and Document Definition updates
123	In/Out	No	Yes	Network Time Protocol (NTP) *recommended*

(1) Access via Port 22 is required only if Barracuda Networks Technical Support is requested.

Activation

Complete the following steps to activate and configure the Barracuda Message Archiver:

1. In the browser address bar enter `http://` followed by the Barracuda Message Archiver IP address, followed by the default web interface HTTP Port `:8000`. For example:
   `http://192.168.200.200:8000`
2. Use the login credentials **admin/admin**
3. In the web interface, you will see the activation warning:

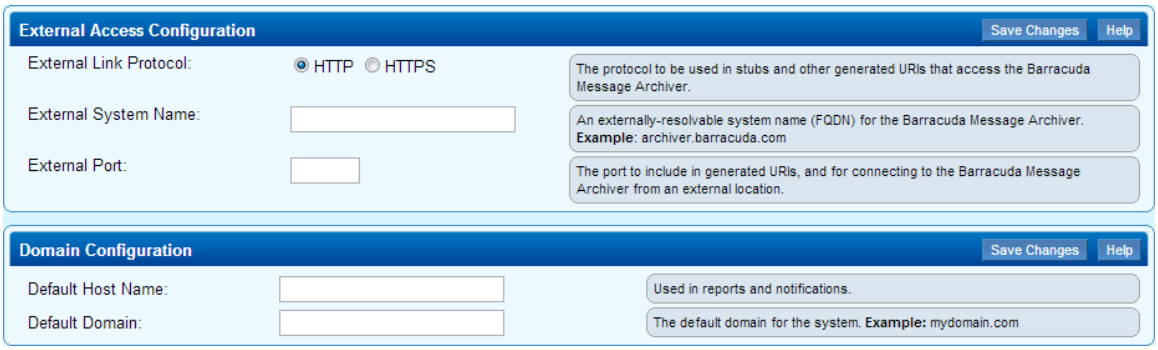
   Error: Activation has not been completed. Please activate your Barracuda Message Archiver to enable functionality. (Click here to activate)
4. Click on the link to open the **Product Activation** page, fill in the required fields, and click **Activate**. The activation process may take up to 15 minutes. A confirmation page displays the terms of your subscription, and the subscription status displays as Activated on the **BASIC > Status** page.
5. Go to **ADVANCED > Firmware Update** page, and download and apply the latest General Release; allow the system to reboot.

Basic and Administration Setup

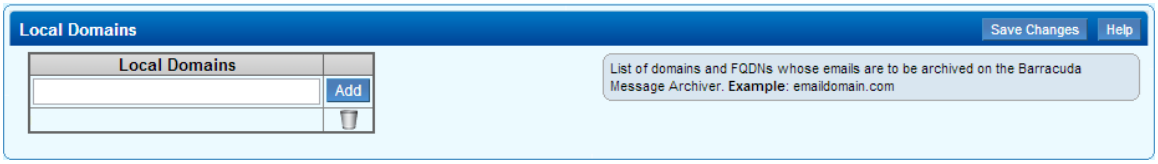
1. Once the system reboots, log back into the web interface.
2. Go to the **BASIC > IP Configuration** tab, and enter the configuration settings including external access configuration and default hostname. In the **External Access Configuration** and **Domain Configuration** sections, complete the following steps; do *not* click **Save Changes** until you complete *both of the following sub steps*:
   - In the **External Access Configuration** section, specify the protocol, and enter the FQDN of your Barracuda Message Archiver for example, archiver.mydomain.com, and enter the port number.

     > ⚠ **External Access – Important**
     > To allow *external* access to the Barracuda Message Archiver, you must enter an *External System Name* and *Port* that are resolvable from outside your organization's internal network. These values are used for stubbing operations and Barracuda Message Archiver Add-In integration.

   - In the **Domain Configuration** section, enter the domains. Note that depending on your environment these may match the FQDN or may be internally registered names:


External Access Configuration
Save Changes
Help
External Link Protocol:
HTTP
HTTPS
The protocol to be used in stubs and other generated URIs that access the Barracuda Message Archiver.
External System Name:
An externally-resolvable system name (FQDN) for the Barracuda Message Archiver. Example: archiver.barracuda.com
External Port:
The port to include in generated URIs, and for connecting to the Barracuda Message Archiver from an external location.
Domain Configuration
Save Changes
Help
Default Host Name:
Used in reports and notifications.
Default Domain:
The default domain for the system. Example: mydomain.com

3. Click **Save Changes** once you have completed *both of the preceding bullet points*.
4. In the **Local Domains** section, include all domains from which to accept mail for archive to identify internal and external email:


Local Domains
Save Changes
Help
Local Domains
Add
List of domains and FQDNs whose emails are to be archived on the Barracuda Message Archiver. Example: emaildomain.com

> Define external access configuration to determine how to integrate with other Barracuda Message Archiver tools and Add-Ins. Define internal or external DNS names depending on how you want to deploy Add-Ins, for example, message stubbing.

5. Go the **BASIC > Administration** page, and configure access, management, and default display settings. For more information, refer to the article How to Configure Administrative Settings.

Enable SMTP Forwarding on the Barracuda Message Archiver

On the Barracuda Message Archiver, go to the **MAIL SOURCES > SMTP/IM** page, and use the following steps to enable SMTP forwarding:

1. In the **SMTP/IM Forwarding Settings** section, set **SMTP/IM Forwarding** to *Yes.*
2. In the **Trusted SMTP Servers** section, enter the IP address of each Microsoft Exchange 2007/2010 Server that is to journal directly to the Barracuda Message Archiver:
    - Exchange 2007 – Add the IP address of *your mailbox server roles*
    - Exchange 2010 – Add all IP addresses of the *Hub Transport server role*

Enable Journaling

To set up journaling, complete the steps described in the article Configuring Envelope (SMTP) Journaling for Microsoft Exchange 2007-2010.

Configure Exchange Integration Operations

1. Log in to the Barracuda Message Archiver web interface, and go to the **MAIL SOURCES > Exchange Integration** page.
2. Click **Start New Action** to define the Exchange actions to execute:
    - **Email Import** – Import all email from your Exchange Server into the Barracuda Message Archiver that meets the specified criteria. Select to import email for all users, or specify import by user name, email address, last name, public folders, or a distribution list.
    - **Non-Email Sync** – Import only non-email Exchange items into the Barracuda Message Archiver from specified accounts including Appointments, Contacts, Tasks, and Notes.
    - **Email Stubbing** – Locate messages on your Exchange Server that meet the specified criteria, copy the specified parts (just attachments, or the entire message with or without attachments) onto the Barracuda Message Archiver, and modify those messages on your Exchange Server so that appropriate parts of the messages are replaced with a stub (a link to where the actual contents reside on the Barracuda Message Archiver).
    - **Folder Sync** – Import into the Barracuda Message Archiver the complete folder structure of the selected users' Mailboxes. This action imports the selected users' custom folders and subfolders.
3. Use the workflow to set up the Exchange action.

> For a comprehensive description of each Exchange Action, go to the **MAIL SOURCES > Exchange Integration** page in the web interface and click **Help**.

Email Service Account Creation

An email service account is a shared account that is accessible by multiple users, allowing the specified users to view and manage email to the account. An email service account allows you to import historical data from your Exchange Server and to manage message attachment stubbing. For details on creating an email service account, refer to the article Creating an Email Service Account for Microsoft Exchange Server 2007/2010.

Next Step: Proceed to the article **Configuring Envelope Journaling for Microsoft Exchange Server 2007 and 2010** to complete your deployment setup.

Understanding Microsoft Exchange Server 2007 and 2010 Envelope Journaling

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher, and a Microsoft® Exchange Server 2007 and 2010.

In this article:

- How Microsoft Exchange Server Journaling Works
- What to Configure

Related Articles

- Configuring Envelope Journaling for Exchange Server 2007/2010
- Message Import, Stubbing & Configuration

Stubbing and Microsoft Exchange Import
For stubbing and Microsoft Exchange imports initiated via the Barracuda Message Archiver web interface, there is a 100MB limit on file import.

Important
If you are migrating to a newer version of Exchange Server, refer to the Barracuda Message Archiver and Microsoft Exchange Server Migration overview for more information.

How Microsoft Exchange Server Journaling Works

Microsoft Exchange Server journaling allows you to record a copy of, or journal, email communications in your organization and send them to a dedicated mailbox on an Exchange Server. The process of journaling is different from archiving. Journaling is simply a means of recording your users' messages. Archiving, on the other hand, is a means of storing those copies in a separate environment for the purpose of regulatory compliance, data retention, or server maintenance.

Microsoft Exchange Server 2007 and 2010 both offer two types of journaling:

- **Standard journaling** - All messages sent *from* or sent *to* addresses on a specific mailbox database are journaled.
- **Premium journaling** - Includes the following options:
  - **Global scope** - All messages that pass through a Hub Transport server are journaled.
  - **Internal scope** - Only messages sent and received within the Exchange organization are journaled.
  - **External scope** - Only messages sent *from* or sent *to* addresses outside the Exchange organization are journaled

Note that each scope within Premium journaling can be further limited by selecting individual *Journal Recipients*. This causes only those messages within a scope that are sent to specific SMTP addresses (mailboxes, contacts, distribution lists) to be journaled. If no recipients are specified, then the scope takes precedence.

Once journaling is enabled on your Exchange Server, it can be configured to forward journaled messages to Message Archiving.

Important
Exchange Server 2007 and 2010 and Message Archiving both support envelope journaling only. This type of journaling copies the body of an email message and its transport envelope information (P2 headers). The envelope information includes the sender and all recipients, including 'bcc' recipients and recipients in distribution lists, which is required data for compliance with most regulations.

Additionally, Exchange cannot fully journal the following:

- **Posts to public folders** - Journaling cannot be enabled on public folder stores.
- **Expansion of external distribution lists** - While the actual contents of messages sent to or from internal and external distribution lists can be journaled, only an internal distribution list can be fully expanded and included in the envelope journaling data. Membership information for a distribution list that is external to your Exchange organization cannot be expanded, and therefore cannot be included in the envelope information even if individual members on the list are in your Exchange server.

What to Configure

To ensure that journaled message archiving begins as soon as your Exchange Servers are configured to send them, register each Exchange Server as a Trusted SMTP Server with the Barracuda Message Archiver (on the **MAIL SOURCES** > **SMTP/IM** page) prior to configuring your Exchange Servers.

Configuring Envelope Journaling for Microsoft Exchange Server 2007 and 2010

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher, and a Microsoft® Exchange Server 2007 and 2010.

In this article:

- Register each Exchange Server as a Trusted SMTP Server
- Configure the Barracuda Message Archiver
- Create a Remote Domain
- Create a Mail Contact
- Create a Send Connector
- Create a Journaling Rule

Related Articles

- Exchange 2007/2010 Envelope Journaling
- Compliance
- Message Import, Stubbing & Configuration
- Understanding SMTP Forwarding and Trusted Servers

Stubbing and Microsoft Exchange Import
For stubbing and Microsoft Exchange imports initiated via the Barracuda Message Archiver web interface, there is a 100MB limit on file import.

If you are migrating to a newer version of Exchange Server, refer to Barracuda Message Archiver and Microsoft Exchange Server Migration.

Depending on your Client Access Licenses (CALs), you may need to apply these rules at the mail server level rather than the hub transport level. For more information, see the Microsoft TechNet article Overview of Compliance Features.

Register each Exchange Server as a Trusted SMTP Server

To ensure that journaled message archiving begins as soon as your Exchange Servers are configured to send them, register each Exchange Server as a Trusted SMTP Server with the Barracuda Message Archiver (on the **MAIL SOURCES** > **SMTP/IM** page) prior to configuring your Exchange Servers.

Once the Barracuda Message Archiver is configured to receive SMTP traffic, you must complete the following from the Exchange Management Console (EMC) of each Exchange Server that will be journaling directly into the Barracuda Message Archiver:

- ***From* Recipient Configuration** - Create a Mail Contact that is to act as the recipient of all journaled messages.
- ***From* Organization Configuration > Hub Transport** - Create the following items:

- a (non-routable) **Remote Domain**, to act as the recipient domain for journaled traffic
- a **Send Connector**, for routing journaled messages
- a **Journaling Rule** to actually enable journaling on your Exchange Server

Configure the Barracuda Message Archiver

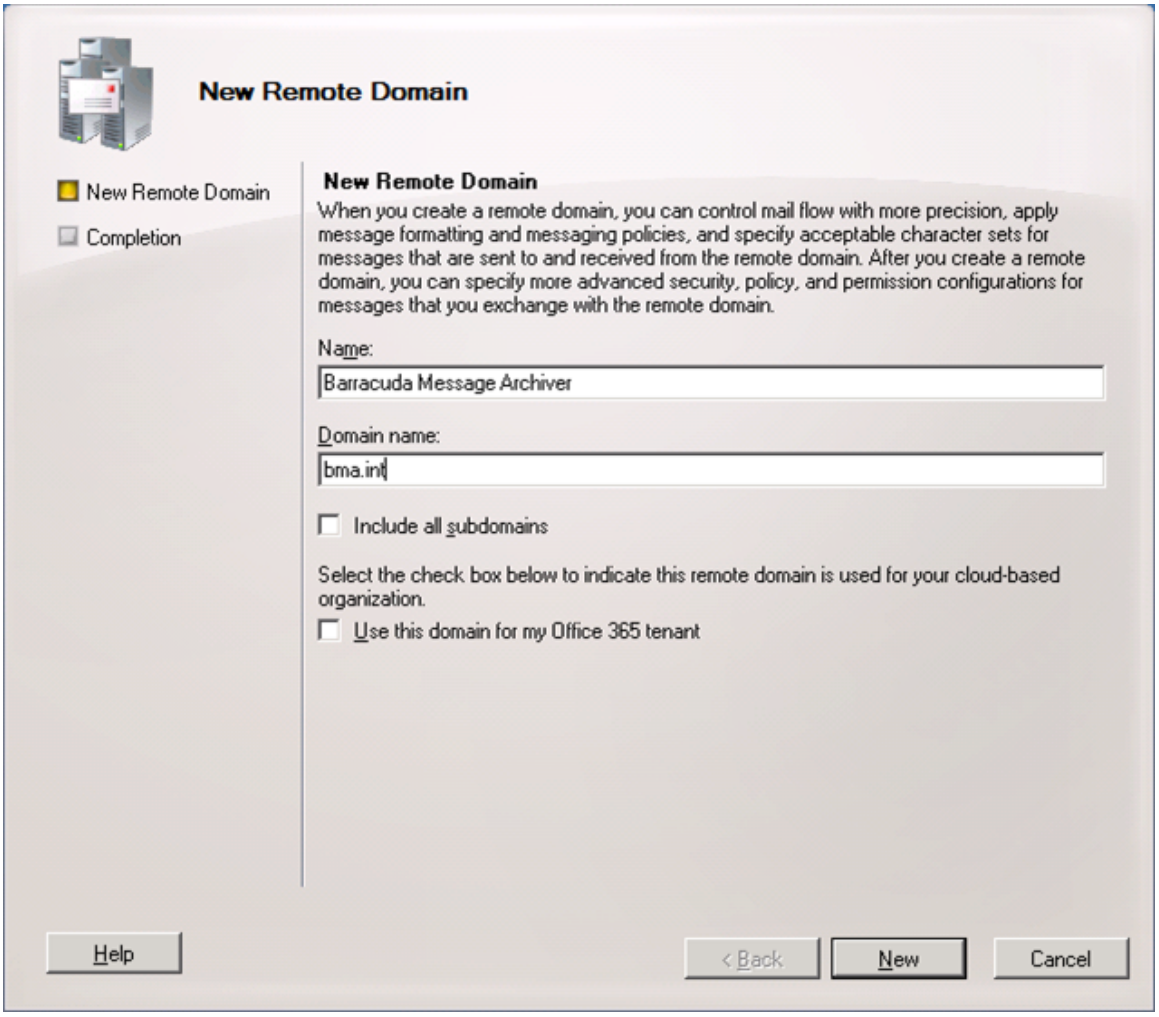
On the Barracuda Message Archiver, use the the following steps to enable SMTP forwarding:

1. Go to the **MAIL SOURCES > SMTP/IM** page.
2. In the **Trusted SMTP Servers** section, enter the IP address of each Exchange Server that is to journal directly to the Barracuda Message Archiver.

Create a Remote Domain

The Remote Domain must be a non-existent or externally non-routable and unresolvable domain, from either inside or outside your organization, and must match the Mail Contact that is the recipient of journaled messages as it is used by the Exchange Server for routing all SMTP Journal traffic. Use the following steps to create a remote domain:

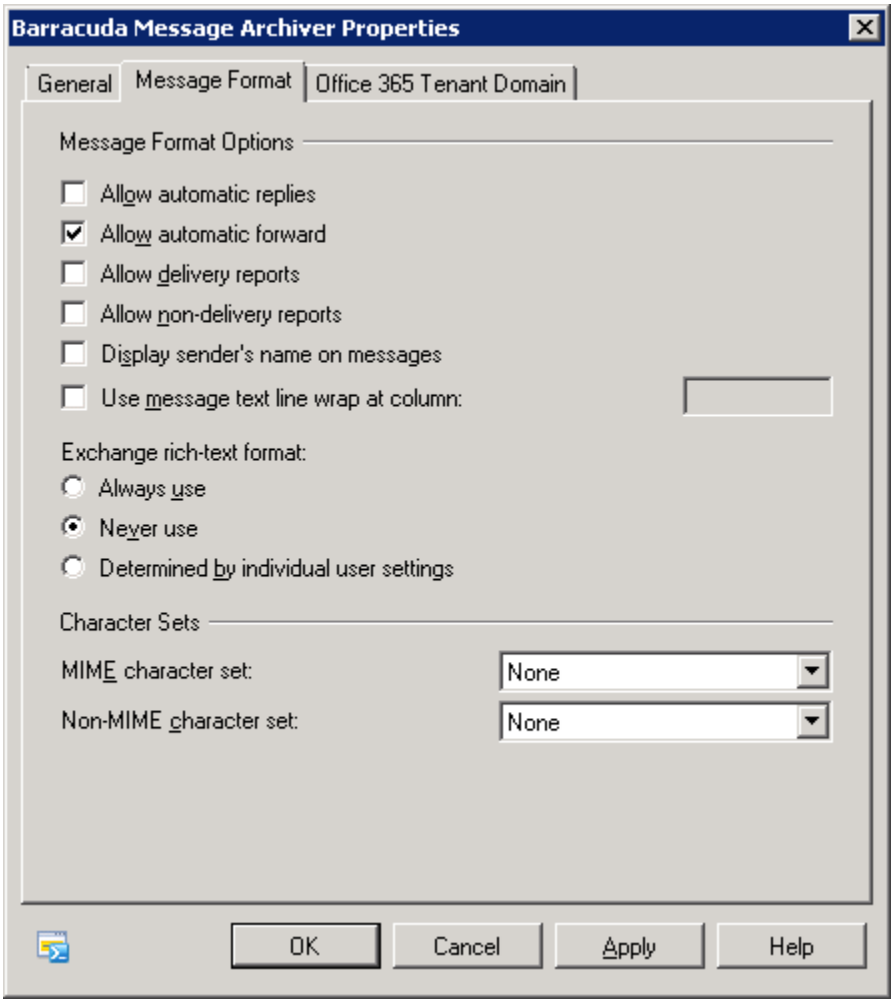
1. Open the **EMC**, expand **Organization Configuration**, select **Hub Transport**, and click the **Remote Domains** tab in the center pane.
2. In the **Actions** panel in the right pane, click **New Remote Domain.** The **New Remote Domain** dialog displays.
3. Enter a **Name** to describe the domain, and the actual **Domain name** you want to use. In this example, *bma.int* is the "fake" domain name that is used. You will use this domain name later when creating the Mail Contact:


New Remote Domain
New Remote Domain
Completion
New Remote Domain
When you create a remote domain, you can control mail flow with more precision, apply message formatting and messaging policies, and specify acceptable character sets for messages that are sent to and received from the remote domain. After you create a remote domain, you can specify more advanced security, policy, and permission configurations for messages that you exchange with the remote domain.
Name:
Barracuda Message Archiver
Domain name:
bma.int
Include all subdomains
Select the check box below to indicate this remote domain is used for your cloud-based organization.
Use this domain for my Office 365 tenant
Help
< Back
New
Cancel

4. Click **New** to verify the domain settings, and click **Finish** to save your settings. The newly created domain displays in the **Remote Domains** list.
5. Double-click on the newly created domain to open the **Properties** dialog for the newly created domain, and:
   - In Exchange 2007, select **Format of original message sent as attachment to the journal report**.
   - In Exchange 2010, select the **Message Format** tab in the **Properties** dialog box.
6. Select the following options to ensure journal messages sent to this domain are *MIME Plain Text* format (rather than the unsupported *Exc*

hange Rich Text format):

- In the **Message Format Options** section, turn on **Allow automatic forward**.
- In the **Exchange rich-text format** section, select **Never Use**:



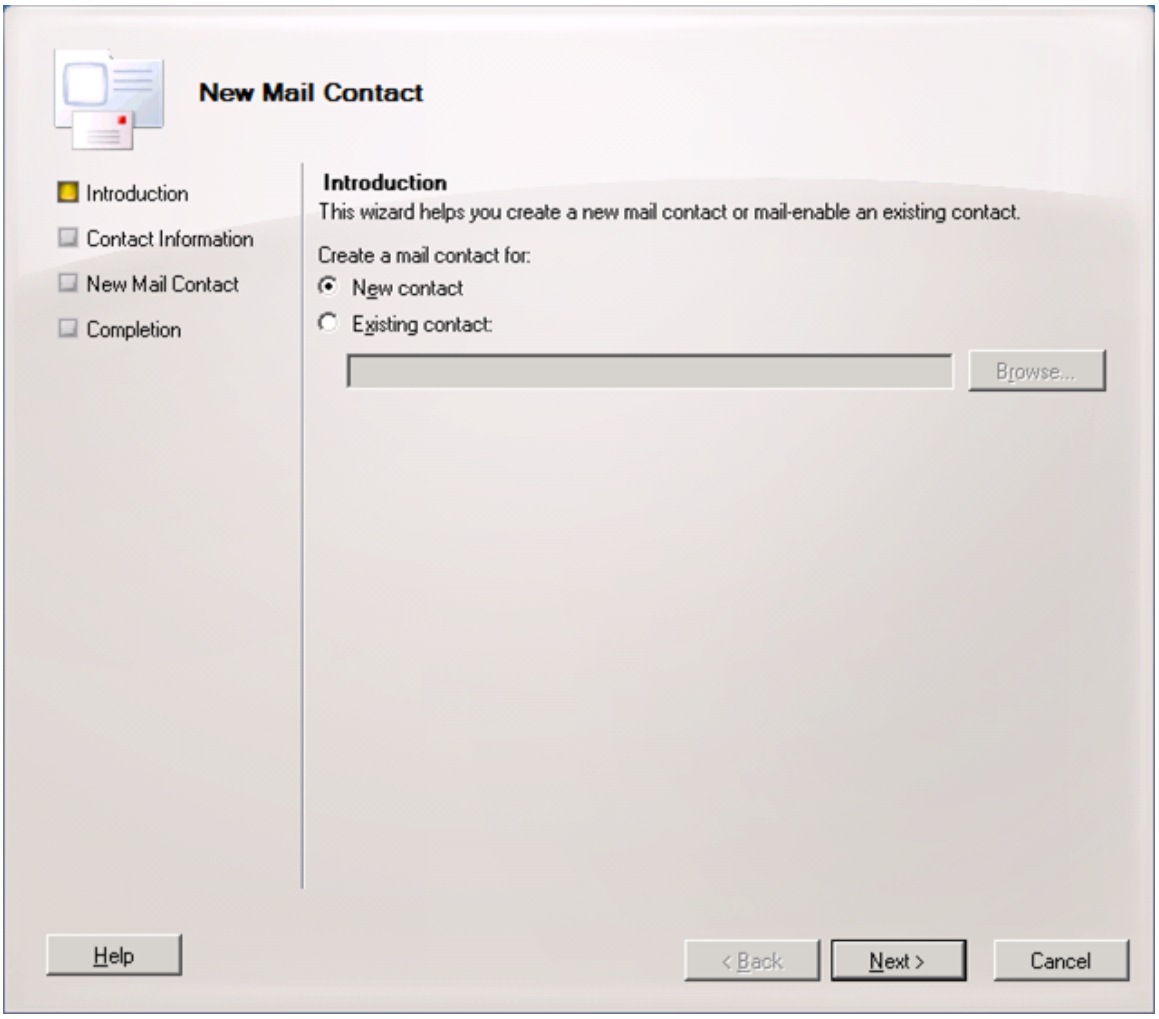
> Verify that only **Never use** and **Allow automatic forward** are selected in the dialog box.

7. Click **Apply** to save your settings, and click **OK** to close the **Properties** dialog.

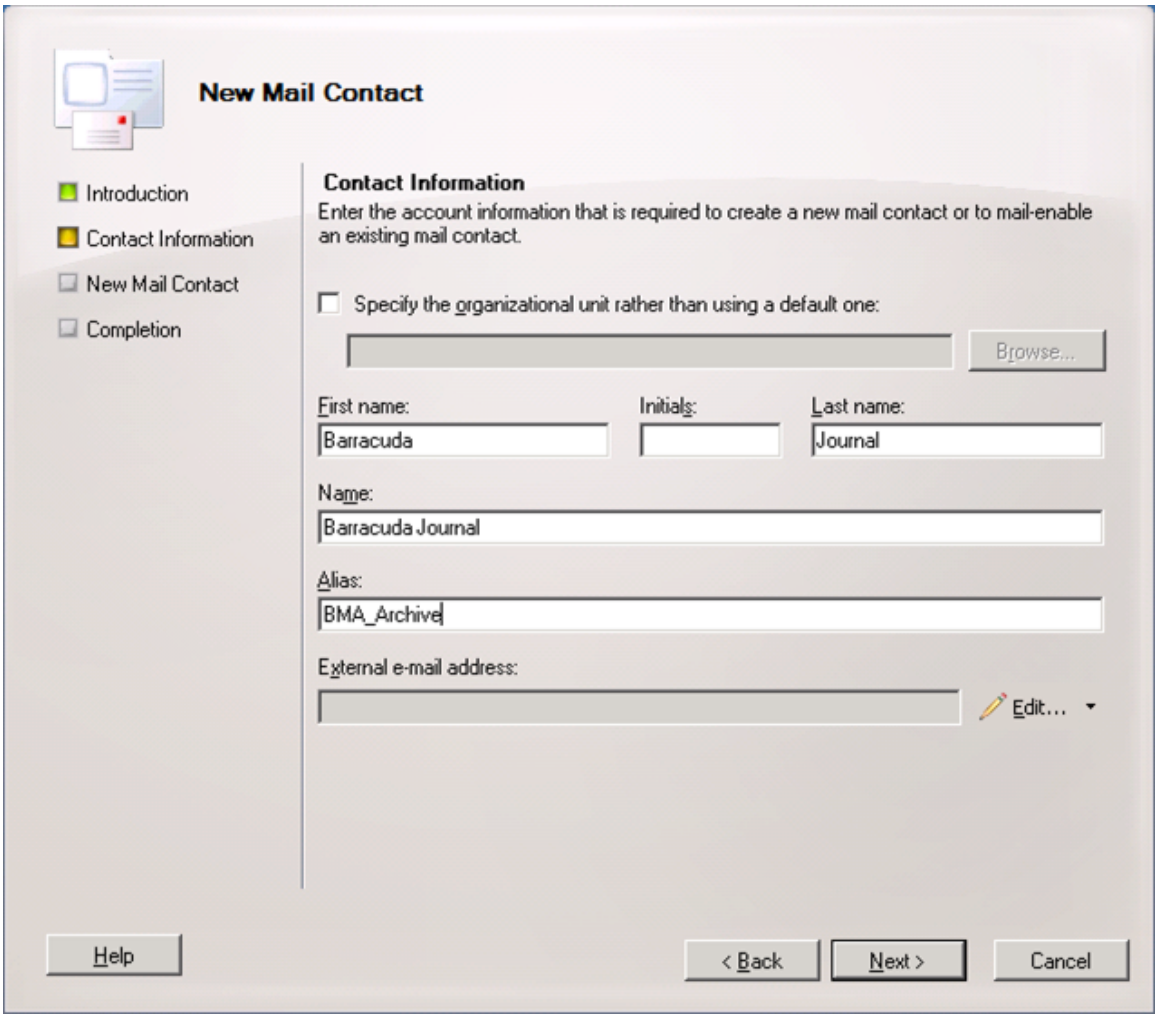
Create a Mail Contact

The Mail Contact is the account that is to act as a "holding location" for journaled messages. The email address associated with this account is the designated recipient, and should be associated with a nonroutable, "dummy" domain name. Use the following steps to create a Mail Contact:

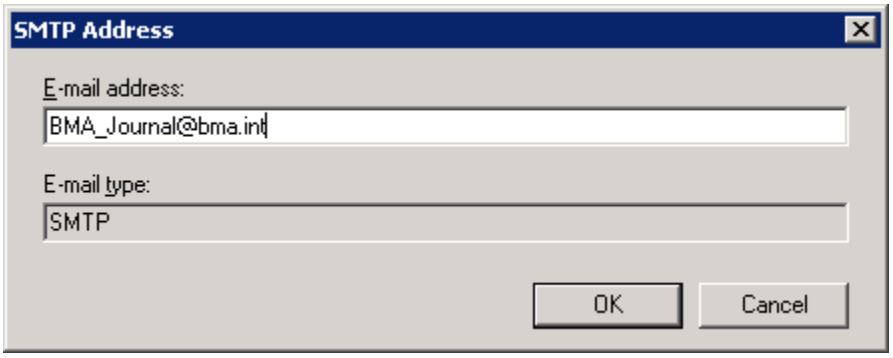
1. In the **EMC**, expand **Recipient Configuration**, select **Mail Contact**, and in the **Actions** panel, click **New Mail Contact**:



2. In the dialog, select **New Contact**, and click **Next**.
3. Enter a **First name** and **Last name**; the **Name** field automatically populates based on the entered values. Enter an **Alias**:

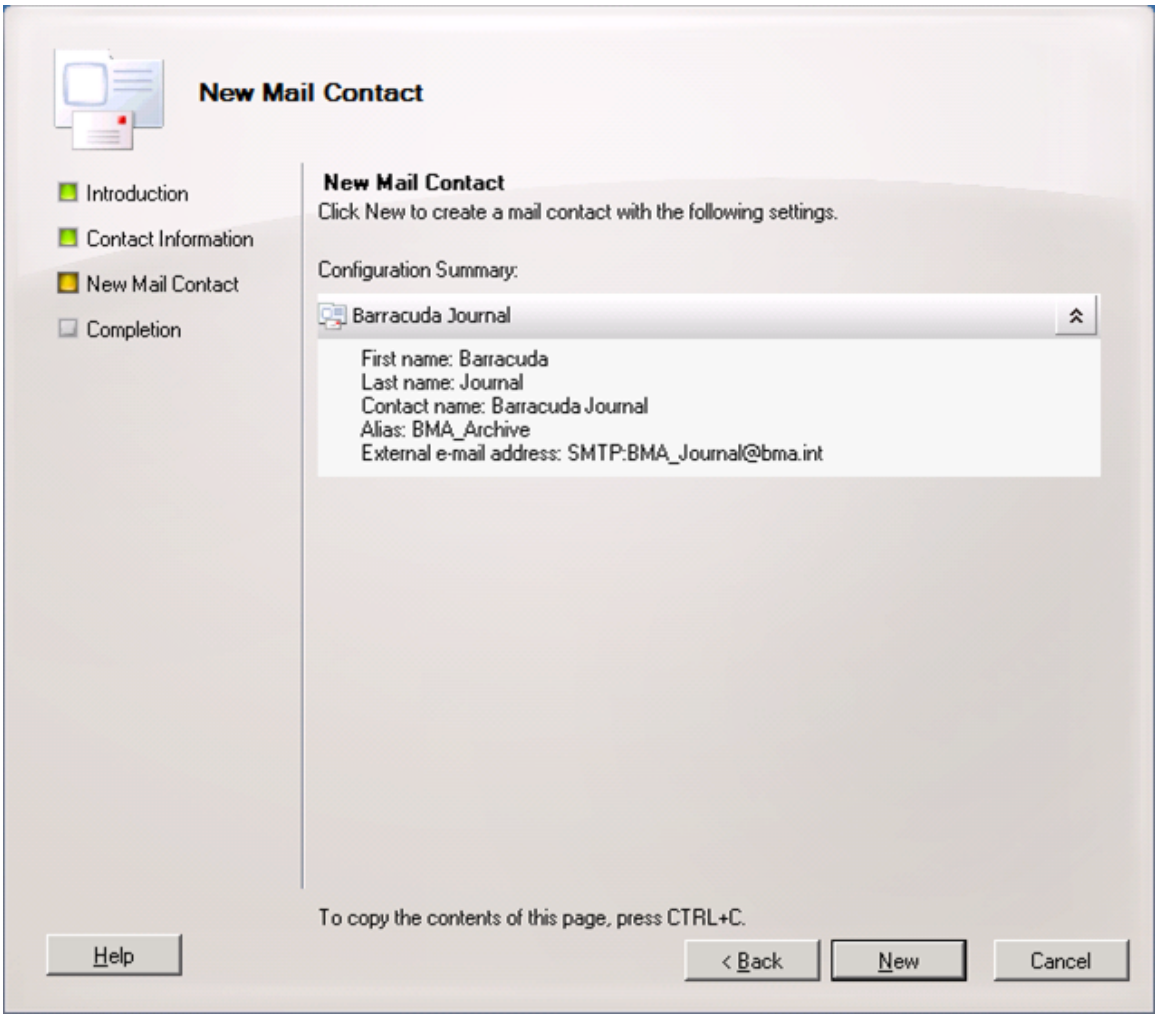


4. Click **Edit** to the right of the **External e-mail address** field, and in the **SMTP Address** dialog, enter the delivery email address, for example, `BMA_Journal@bma.int`:



> The account name can be anything you want, but the domain name *must match* what you created in the preceding section, **Create a Remote Domain**.

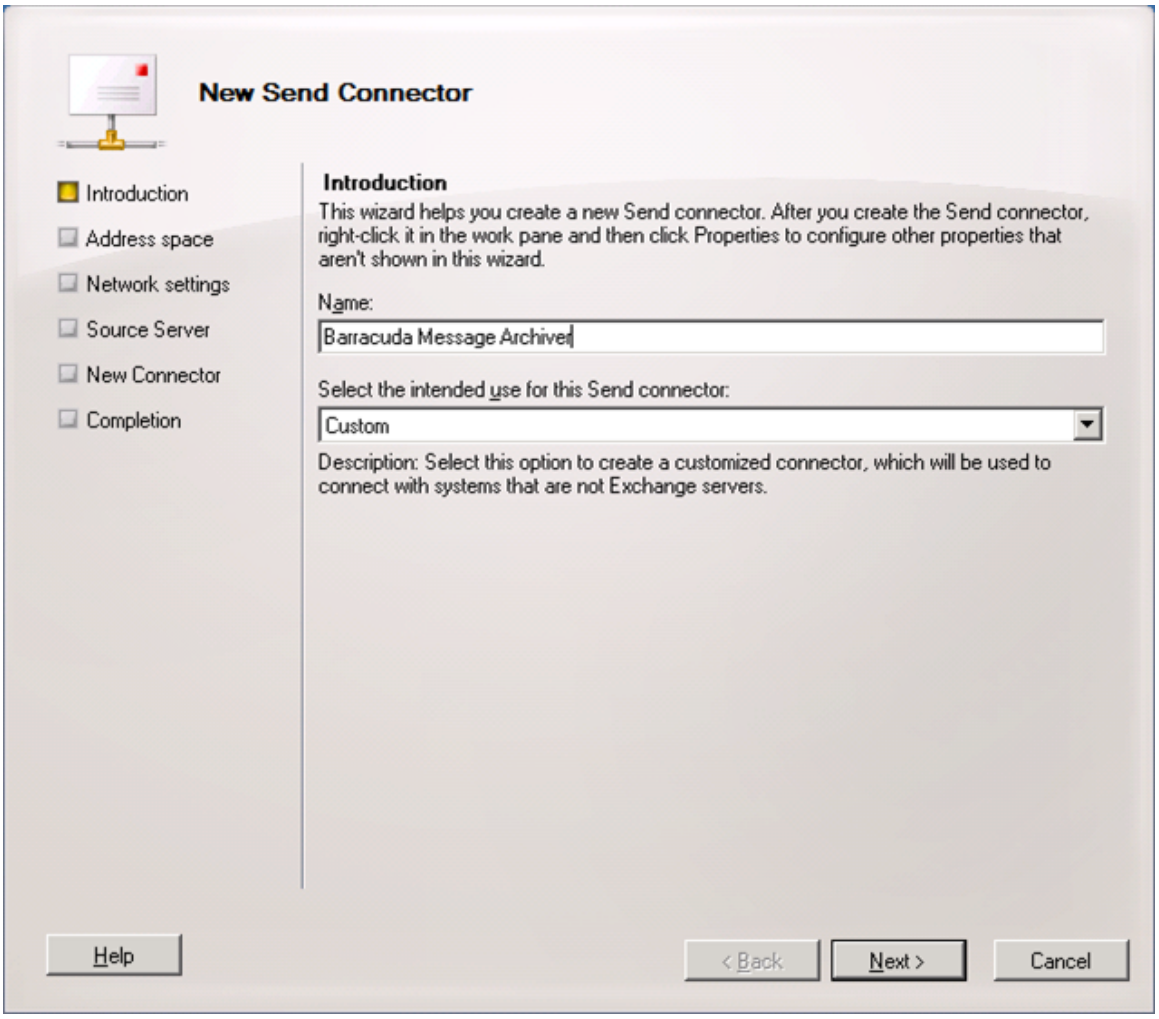
5. Click **OK** to close the dialog box. In the Wizard, click **Next** to verify the information:



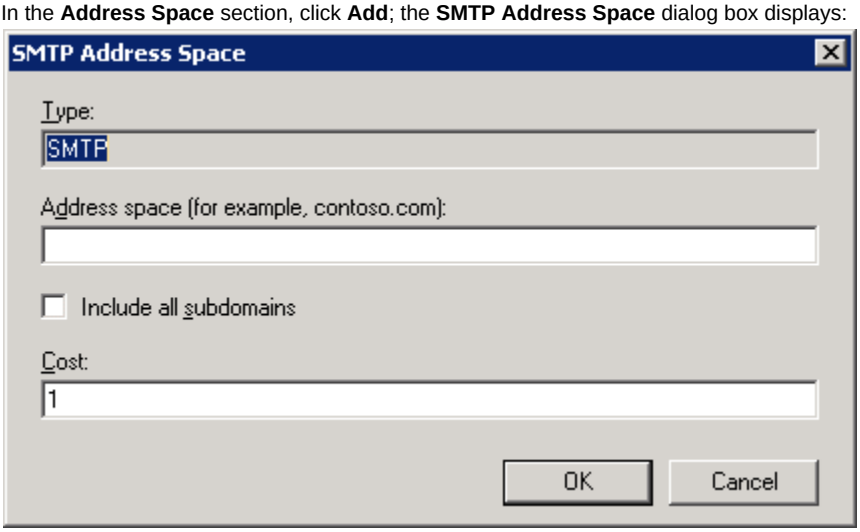
6. Click **New** to create the Mail Contact. The newly-created contact appears in the **Mail Contact** list. Click **Finish** to close the Wizard.

Create a Send Connector

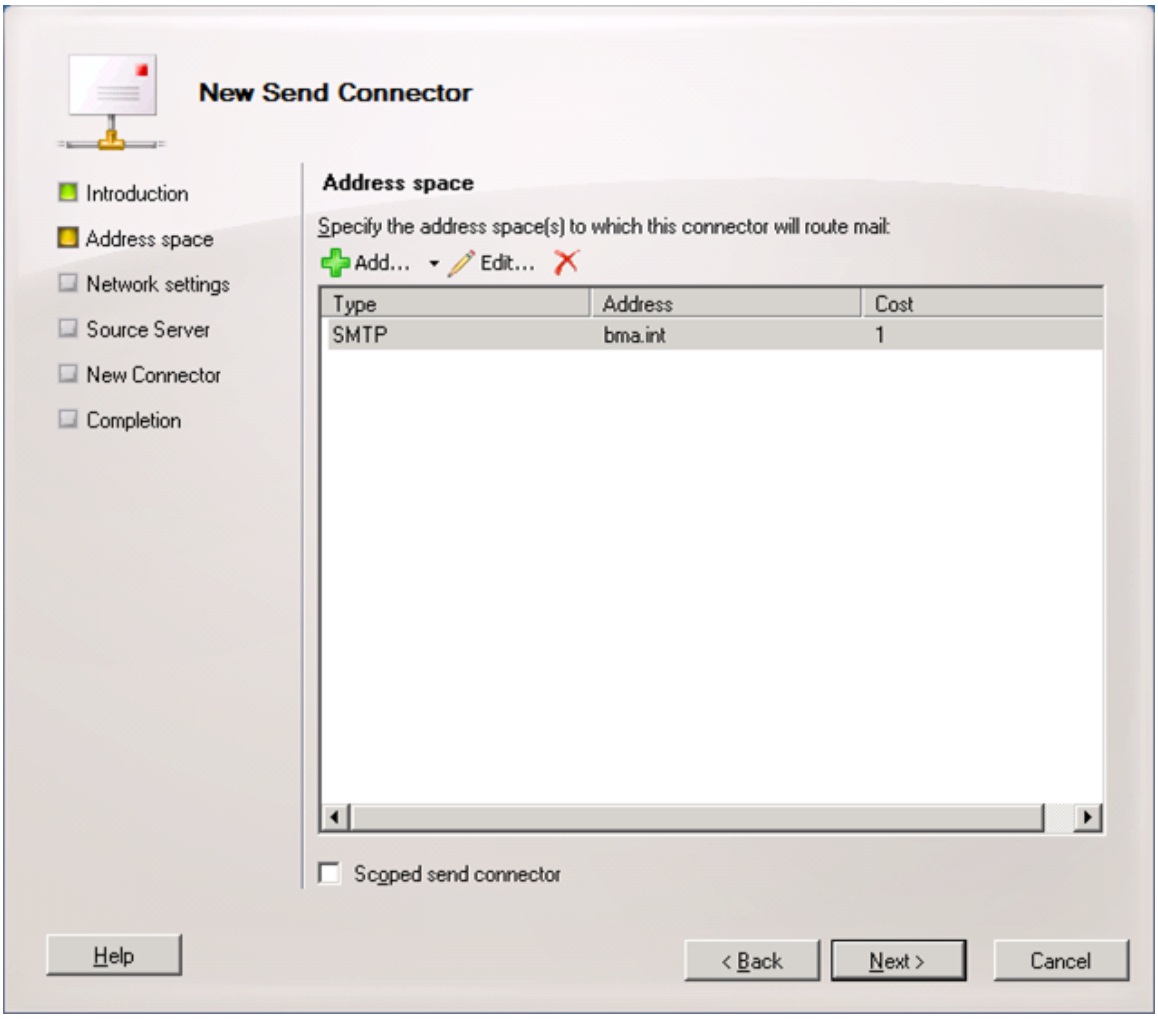
1. In the **EMC**, expand **Organization Configuration**, select **Hub Transport**, and select the **Send Connector** tab. In the **Actions** panel, and click **New Send Connector**. The **New Send Connector** dialog displays. Enter a **Name** to identify this send connector, e.g., `Barracuda Message Archiver`:


New Send Connector
Introduction
Address space
Network settings
Source Server
New Connector
Completion
Introduction
This wizard helps you create a new Send connector. After you create the Send connector, right-click it in the work pane and then click Properties to configure other properties that aren't shown in this wizard.
Name:
Barracuda Message Archiver
Select the intended use for this Send connector:
Custom
Description: Select this option to create a customized connector, which will be used to connect with systems that are not Exchange servers.
Help
< Back
Next >
Cancel

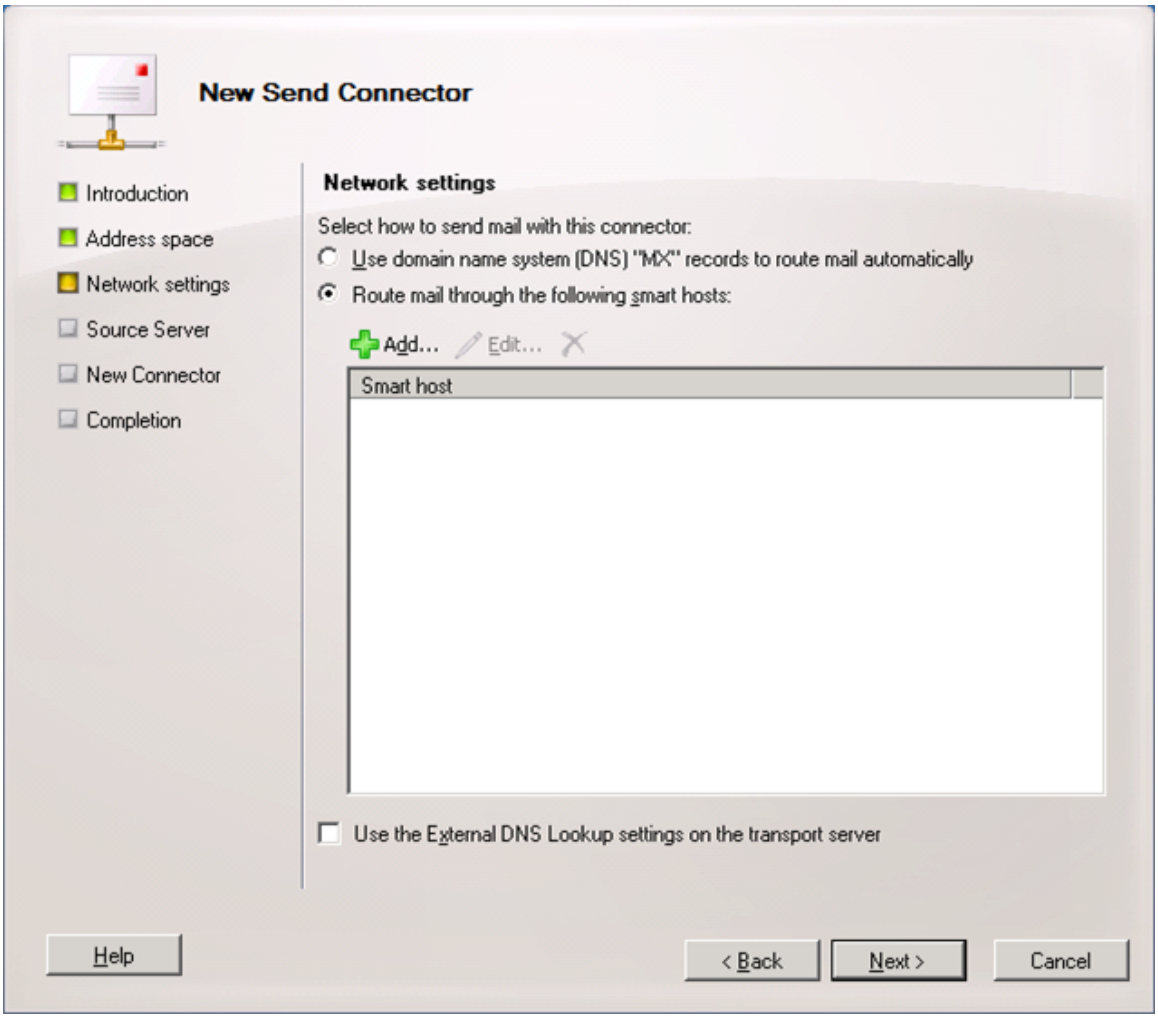
2. From the **Select the intended use for this Send connector** menu, select **Custom**, and click **Next**.
3. In the **Address Space** section, click **Add**; the **SMTP Address Space** dialog box displays:



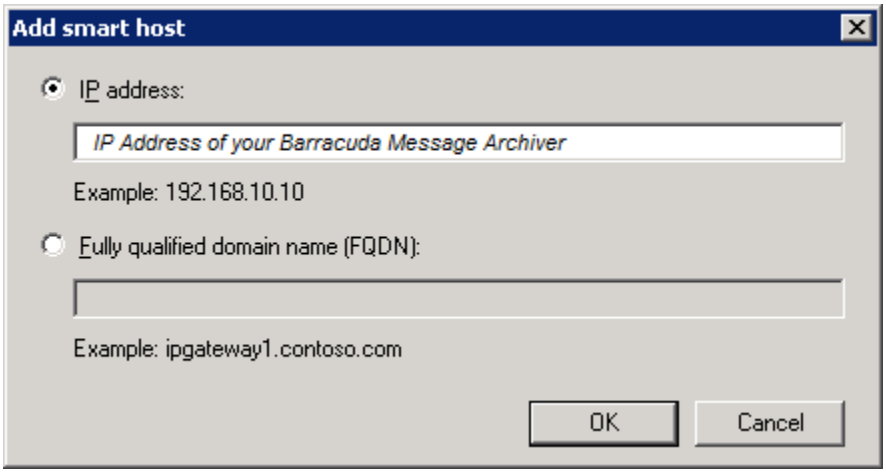
4. In the **Address space** field, enter the domain created earlier, e.g., `bma.int`, and click **OK**. The SMTP connector is added:



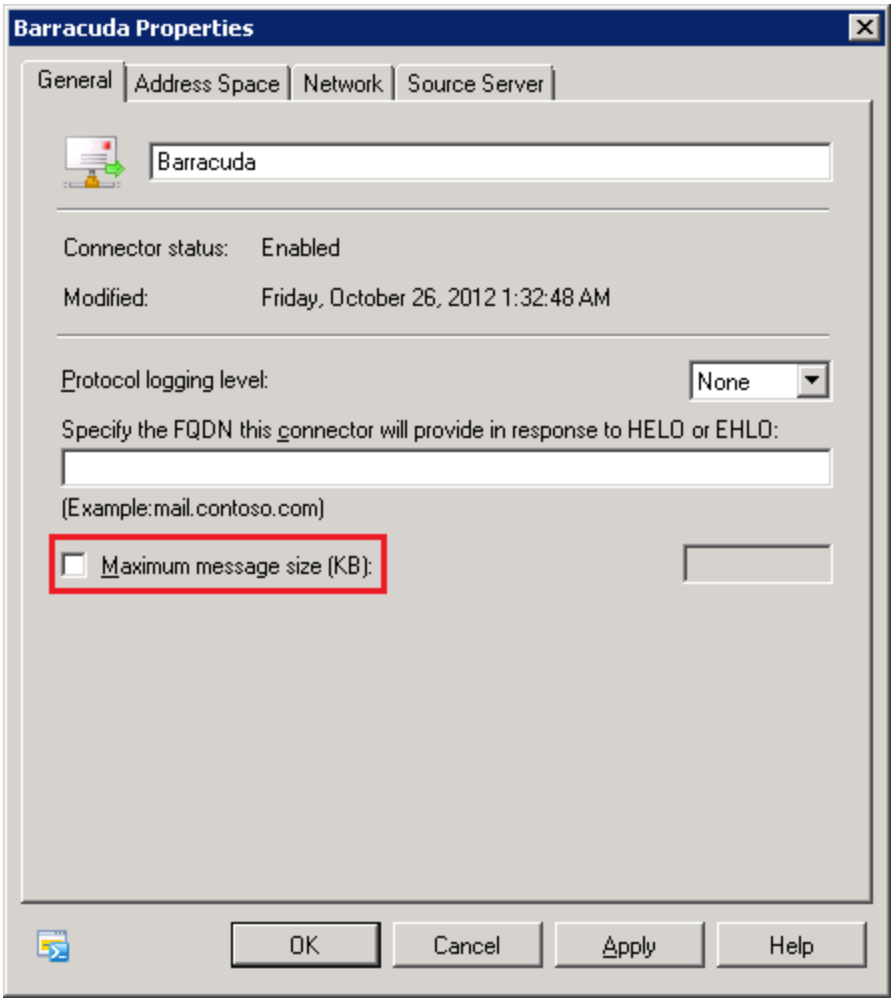
5. Click **Next**. Select **Route mail through the following smart host**:



6. Click **Add**. In the **Add smart host** dialog box, select **IP address**, and enter the IP address of your Barracuda Message Archiver:



7. Click **OK** to add the IP address. Click **Next**, then click **Next** again.
8. In the **Source Server** page, if your Exchange server is not already listed, click **Add** to search for and add the server to this list. Click **Next** to verify your configuration, and click **New** to create the Send Connector. Click **Finish** to return to the **Send Connectors** tab; the newly-created Send Connector displays in the list.
9. Right-click on the new Send Connector, and click **Properties**.
10. In the **Properties** dialog box, clear **Maximum message size (KB)**:

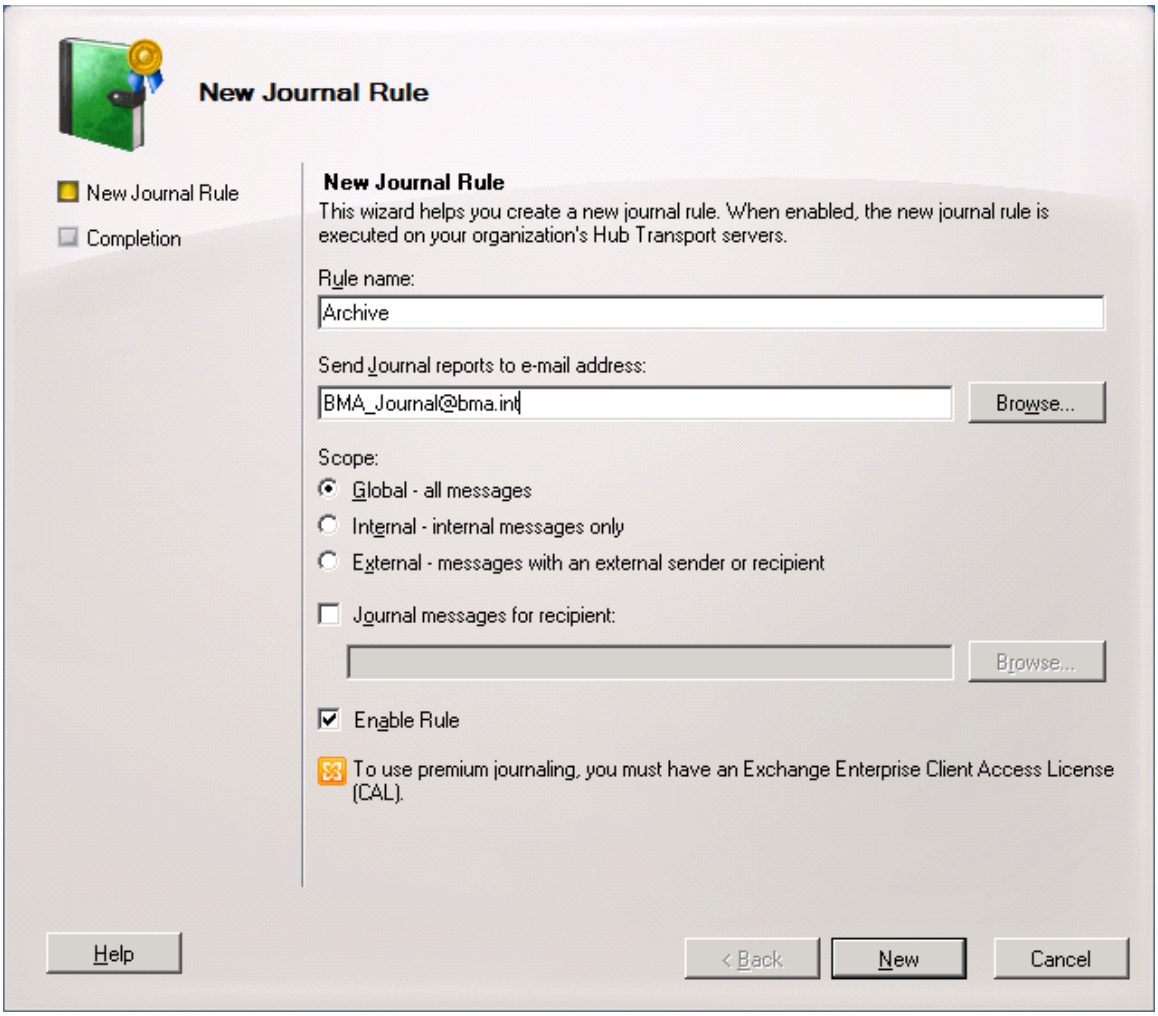


11. Click **Apply**, and then click **OK** to save your changes and close the dialog box.

Create a Journaling Rule

Both the Standard and Enterprise versions of Microsoft Exchange Server 2007 and 2010 support Standard and Premium Journaling. Open the EMC, and complete the following steps to add a journaling rule:

1. In the **EMC**, expand **Organization Configuration**, select **Hub Transport**, and select the **Journal Rules** tab.
2. In the **Actions** panel, click **New Journal Rule**; the **New Journal Rule** dialog displays.
3. Enter a Rule name, and for the **Send Journal reports to e-mail address**, click **Browse** and navigate to and select the mail contact created in the section **Create a Mail Contact**; e.g., `BMA_Journal@bma.int`:


New Journal Rule
New Journal Rule
Completion
New Journal Rule
This wizard helps you create a new journal rule. When enabled, the new journal rule is executed on your organization's Hub Transport servers.
Rule name:
Archive
Send Journal reports to e-mail address:
BMA_Journal@bma.int
Browse...
Scope:
Global - all messages
Internal - internal messages only
External - messages with an external sender or recipient
Journal messages for recipient:
Browse...
Enable Rule
To use premium journaling, you must have an Exchange Enterprise Client Access License (CAL).
Help
< Back
New
Cancel

4. Select the Scope for archiving; the recommended setting is **Global - all messages** for the most complete coverage.
5. Turn on **Enable Rule**, click **New** to create the Journaling rule, and click **Finish** to return to the **Journal Rules** tab where the newly-created rule displays in the list.

Configuring an IMAP or POP3 Journal Account for Microsoft Exchange Server 2007 and 2010

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher, and Microsoft® Exchange Server 2007 and 2010.

Barracuda Networks recommends deploying your Barracuda Message Archiver with Microsoft Exchange Server 2007/2010 using the push method, alternately, you can set up IMAP or POP3 journal accounts as described in this article.

You can configure the Barracuda Message Archiver to automatically retrieve messages directly from your mail server using the IMAP or POP3 protocol.

In this article:

- Service Availability
- Start the Service
- Add a Journal Account to the Barracuda Message Archiver

Related Articles

- Envelope Journaling for Exchange 2007/2010

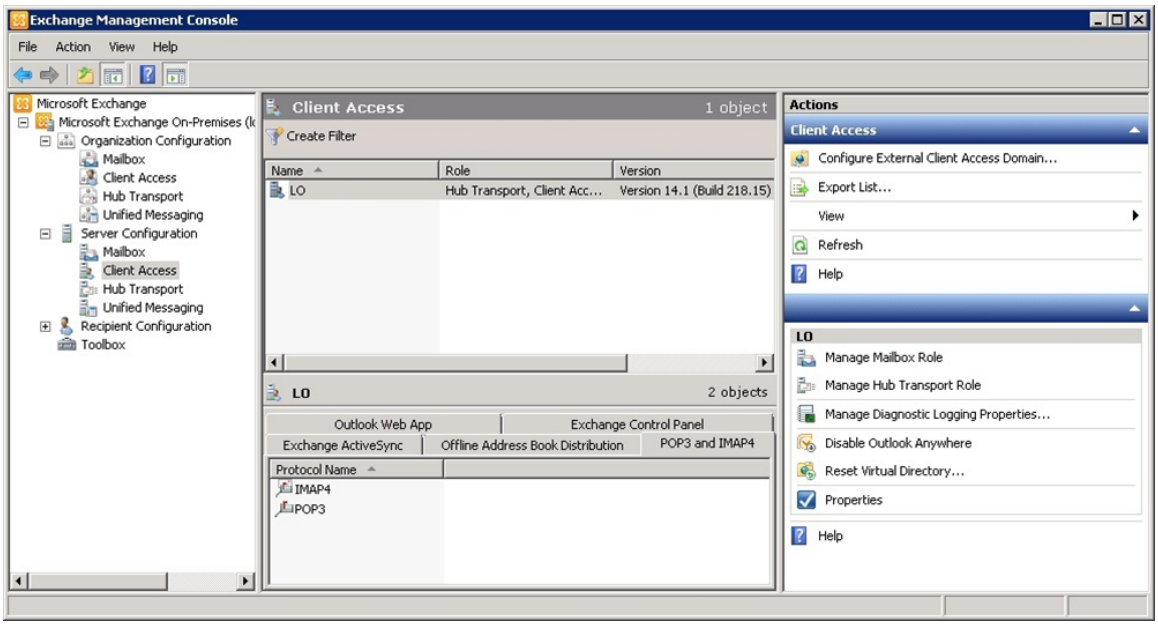
Important
If you are migrating to a newer version of Exchange Server, refer to Barracuda Message Archiver and Microsoft Exchange Server

Migration.

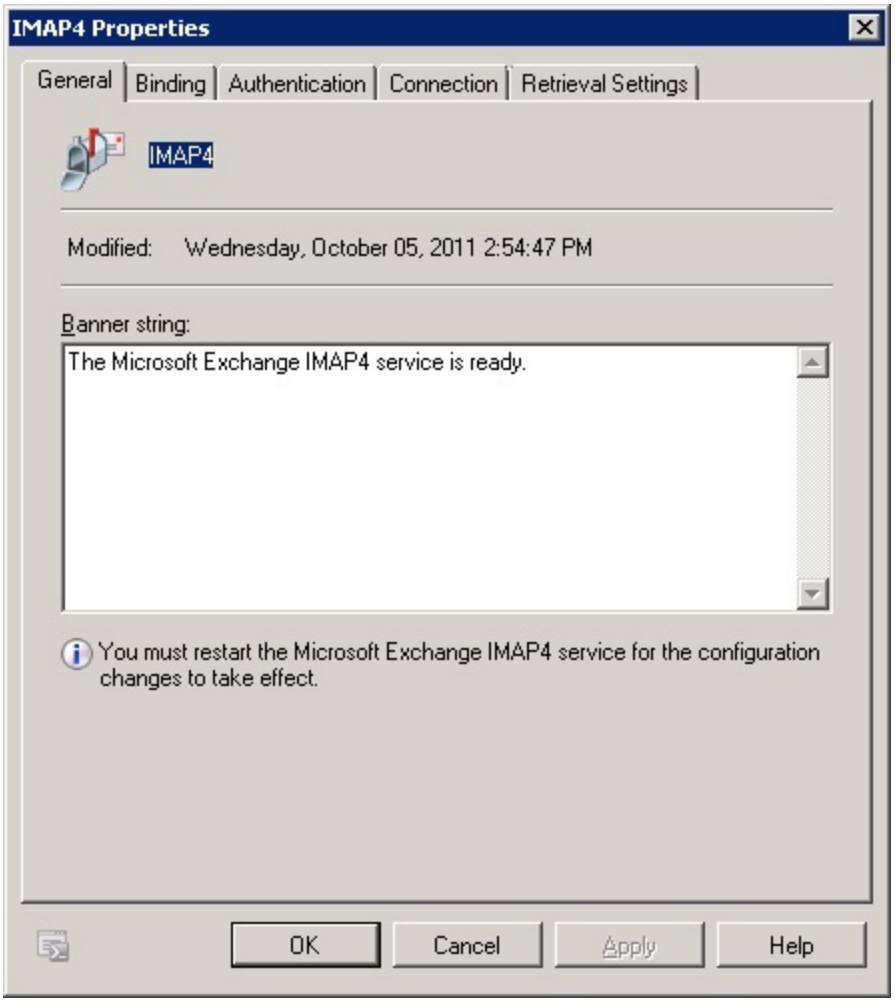
Service Availability

Use the following steps to verify the IMAP or POP3 service is available on the Exchange Server.

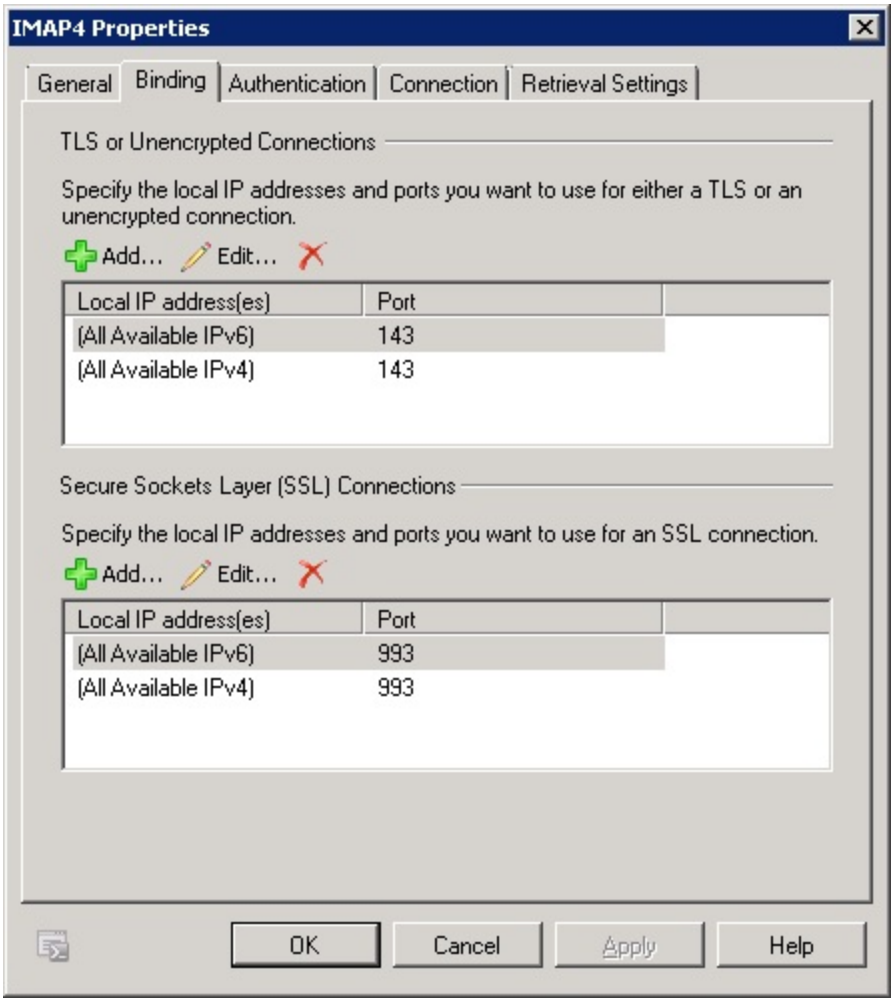
1. Log in to the Exchange Server as the Exchange Server Administrator.
2. Go to **All Programs > Microsoft Exchange Server > Exchange Management Console**.
3. In the Console tree, navigate to and click **Client Access**.
4. In the **Work** pane, click the **POP 3 and IMAP 4** tab:



5. Right-click on the desired service, for example, **IMAP4**, and click **Properties**.
6. In the **General** tab, verify the service is "ready" in the **Banner string** window:



7. Click the **Binding** tab to view the default port for the service:

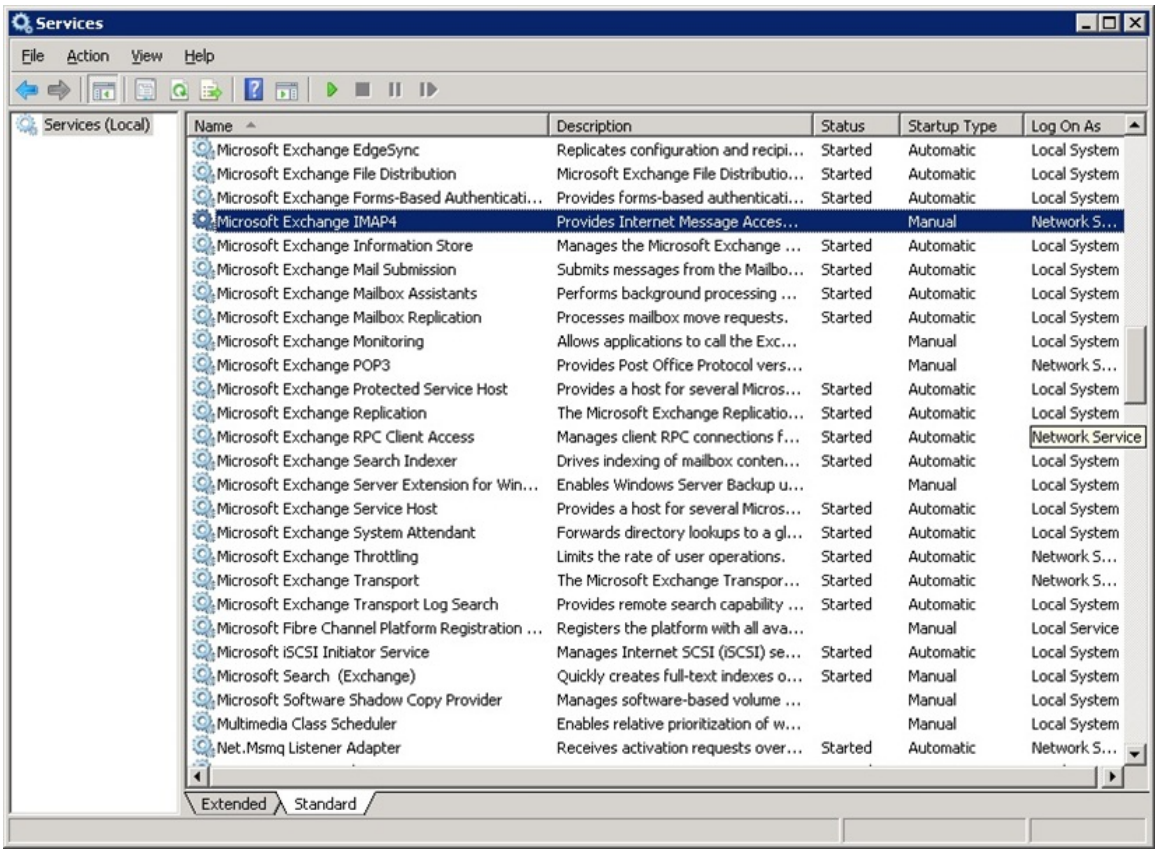


8. To modify the port number, select from the available options:
    - **Add** - Click to add an additional port number
    - **Edit** - Click to modify the port details for the highlighted item
    - **Delete** - Click to remove the highlighted port from the list
9. Click **OK** to save your changes and close the dialog box.

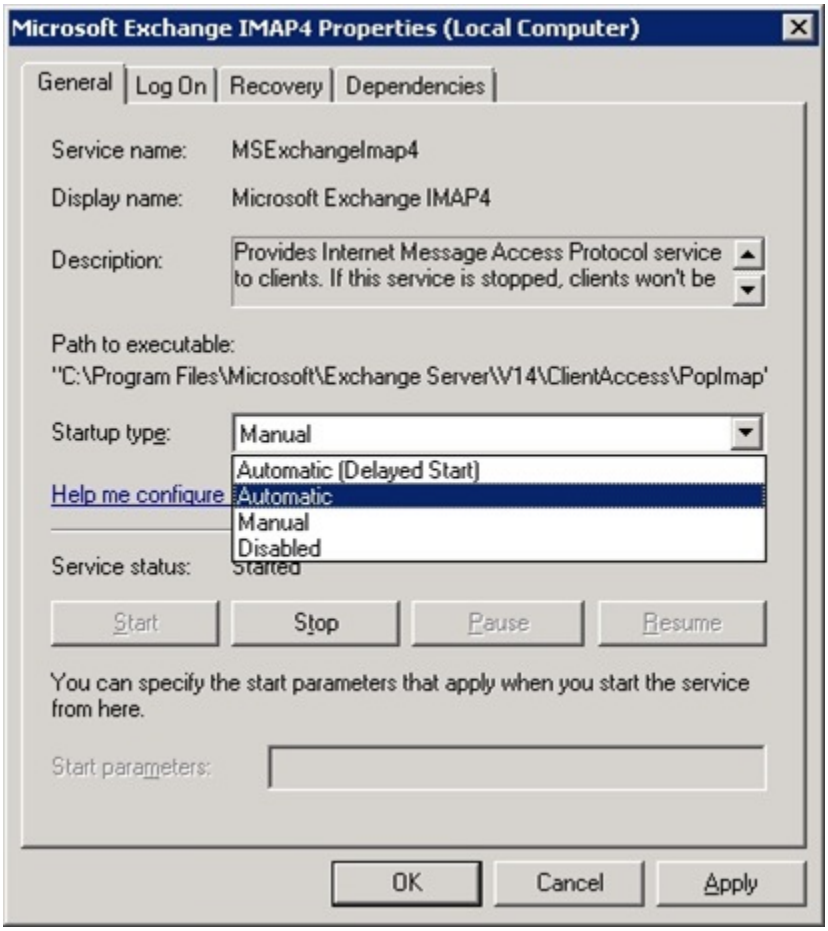
Start the Service

Use the following steps to start the service.

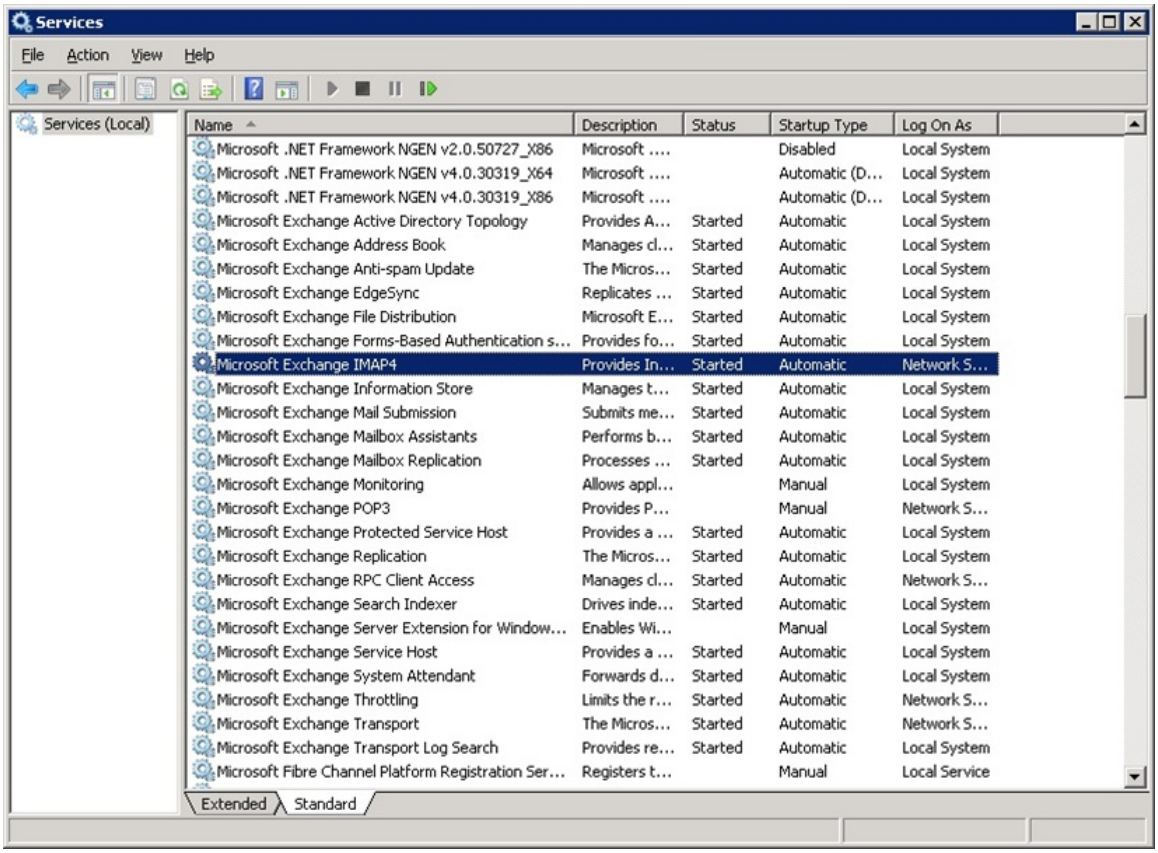
1. Log in to the Exchange Server as the Exchange Server Administrator, and go to **Start > Programs > Administrative Tools > Services**.
2. Locate and click the desired service in the **Services** window, for example, **Microsoft Exchange IMAP 4**:


Services
File Action View Help
Services (Local)
Name Description Status Startup Type Log On As
Microsoft Exchange EdgeSync Replicates configuration and recipi... Started Automatic Local System
Microsoft Exchange File Distribution Microsoft Exchange File Distributio... Started Automatic Local System
Microsoft Exchange Forms-Based Authenticati... Provides forms-based authenticati... Started Automatic Local System
Microsoft Exchange IMAP4 Provides Internet Message Acces... Manual Network S...
Microsoft Exchange Information Store Manages the Microsoft Exchange ... Started Automatic Local System
Microsoft Exchange Mail Submission Submits messages from the Mailbo... Started Automatic Local System
Microsoft Exchange Mailbox Assistants Performs background processing ... Started Automatic Local System
Microsoft Exchange Mailbox Replication Processes mailbox move requests. Started Automatic Local System
Microsoft Exchange Monitoring Allows applications to call the Exc... Manual Local System
Microsoft Exchange POP3 Provides Post Office Protocol vers... Manual Network S...
Microsoft Exchange Protected Service Host Provides a host for several Micros... Started Automatic Local System
Microsoft Exchange Replication The Microsoft Exchange Replicatio... Started Automatic Local System
Microsoft Exchange RPC Client Access Manages client RPC connections f... Started Automatic Network Service
Microsoft Exchange Search Indexer Drives indexing of mailbox conten... Started Automatic Local System
Microsoft Exchange Server Extension for Win... Enables Windows Server Backup u... Manual Local System
Microsoft Exchange Service Host Provides a host for several Micros... Started Automatic Local System
Microsoft Exchange System Attendant Forwards directory lookups to a gl... Started Automatic Local System
Microsoft Exchange Throttling Limits the rate of user operations. Started Automatic Network S...
Microsoft Exchange Transport The Microsoft Exchange Transpor... Started Automatic Network S...
Microsoft Exchange Transport Log Search Provides remote search capability ... Started Automatic Local System
Microsoft Fibre Channel Platform Registration ... Registers the platform with all ava... Manual Local Service
Microsoft iSCSI Initiator Service Manages Internet SCSI (iSCSI) se... Started Automatic Local System
Microsoft Search (Exchange) Quickly creates full-text indexes o... Started Manual Local System
Microsoft Software Shadow Copy Provider Manages software-based volume ... Manual Local System
Multimedia Class Scheduler Enables relative prioritization of w... Manual Local System
Net.Msmq Listener Adapter Receives activation requests over... Started Automatic Network S...
Extended Standard

3. Right-click on the service name, and click **Properties**.
4. In the **Properties** dialog box, select **Automatic** from the **Startup type** drop-down menu:


Microsoft Exchange IMAP4 Properties (Local Computer)
General Log On Recovery Dependencies
Service name: MSExchangeImap4
Display name: Microsoft Exchange IMAP4
Description: Provides Internet Message Access Protocol service to clients. If this service is stopped, clients won't be
Path to executable:
"C:\Program Files\Microsoft\Exchange Server\V14\ClientAccess\PopImap"
Startup type: Manual
Automatic (Delayed Start)
Automatic
Manual
Disabled
Help me configure
Service status: Started
Start Stop Pause Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK Cancel Apply

5. Click **Start**, and then click **OK** to save your settings.
6. In the **Services** window, verify the Status is **Started** and the **Startup Type** is **Automatic**:


Services
File Action View Help
Services (Local)
Name | Description | Status | Startup Type | Log On As
Microsoft .NET Framework NGEN v2.0.50727_X86 | Microsoft .... | | Disabled | Local System
Microsoft .NET Framework NGEN v4.0.30319_X64 | Microsoft .... | | Automatic (D... | Local System
Microsoft .NET Framework NGEN v4.0.30319_X86 | Microsoft .... | | Automatic (D... | Local System
Microsoft Exchange Active Directory Topology | Provides A... | Started | Automatic | Local System
Microsoft Exchange Address Book | Manages cl... | Started | Automatic | Local System
Microsoft Exchange Anti-spam Update | The Micros... | Started | Automatic | Local System
Microsoft Exchange EdgeSync | Replicates ... | Started | Automatic | Local System
Microsoft Exchange File Distribution | Microsoft E... | Started | Automatic | Local System
Microsoft Exchange Forms-Based Authentication s... | Provides fo... | Started | Automatic | Local System
Microsoft Exchange IMAP4 | Provides In... | Started | Automatic | Network S...
Microsoft Exchange Information Store | Manages t... | Started | Automatic | Local System
Microsoft Exchange Mail Submission | Submits me... | Started | Automatic | Local System
Microsoft Exchange Mailbox Assistants | Performs b... | Started | Automatic | Local System
Microsoft Exchange Mailbox Replication | Processes ... | Started | Automatic | Local System
Microsoft Exchange Monitoring | Allows appl... | | Manual | Local System
Microsoft Exchange POP3 | Provides P... | | Manual | Network S...
Microsoft Exchange Protected Service Host | Provides a ... | Started | Automatic | Local System
Microsoft Exchange Replication | The Micros... | Started | Automatic | Local System
Microsoft Exchange RPC Client Access | Manages cl... | Started | Automatic | Network S...
Microsoft Exchange Search Indexer | Drives inde... | Started | Automatic | Local System
Microsoft Exchange Server Extension for Window... | Enables Wi... | | Manual | Local System
Microsoft Exchange Service Host | Provides a ... | Started | Automatic | Local System
Microsoft Exchange System Attendant | Forwards d... | Started | Automatic | Local System
Microsoft Exchange Throttling | Limits the r... | Started | Automatic | Network S...
Microsoft Exchange Transport | The Micros... | Started | Automatic | Network S...
Microsoft Exchange Transport Log Search | Provides re... | Started | Automatic | Local System
Microsoft Fibre Channel Platform Registration Ser... | Registers t... | | Manual | Local Service
Extended Standard

7. Close the **Services** window.

Add a Journal Account to the Barracuda Message Archiver

Once you configure the Service on your Exchange Server, you can add the journal account to the Barracuda Message Archiver to begin retrieving new messages for archiving.

1. Log in to the Barracuda Message Archiver as the administrator, and go to **MAIL SOURCES > Journal Accounts**.
2. In the **Journal Accounts** section, enter the following details:
    - **Enable Journal Accounts** - Select **Yes** to allow the Barracuda Message Archiver to poll the listed accounts for new messages for archiving.
    - **Enable Journal** - When set to **Yes**, all listed accounts are tested for connectivity with each page view**.**
    - **Polling Frequency** - Specify how often to poll each journal account for new messages
3. In the **Journal Accounts Configuration** section, specify the following details for each journal account:
    - **Status** - Displays the connection status for each account.
    - **Server** - Enter the hostname of the mail server where the account resides.
    - **Protocol** - Select whether the account is POP3 or IMAP; once you select the protocol, the default port number automatically populates the **Port** field.
    - **Username** - Enter the username or ID associated with this mailbox as defined by your server. This is usually the mailbox designated as the "journaling" email address on your mail server, and specified by the complete email address such as **journal @example.com**.
    - **Password** - Enter the password associated with the username.
    - **Encryption**–Select the type of encryption used to connect to the mail server:
        - **TLS (if available)**
        - **TLS**
        - **SSL**
        - **None**
    - **Port**–Select the associated port based on the selected protocol; the default value is port 143 for **IMAP**, and port 110 for **POP3**.
4. **Keep Items on Server**:
    - Select **Off** to allow the Barracuda Message Archiver to automatically clean up the contents of the journal mailbox after each import.

- Select **On** to prevent the Barracuda Message Archiver from removing the journaled messages from the mail server; *only* turn this option on if the contents of the journal account is required by other applications. In this case, make sure that another method for cleaning up the journal account is enabled on the mail server in order to prevent unlimited growth on the mail server and to stay in compliance with your organization's message retention policies.

  > Barracuda Networks recommends that you set the value of **keep Items on Server** to **Off** to save hard drive space on your mail server.

5. Click **Add** to add the journal account; verify the **Status** field displays green, and then click **Save Changes**.
6. To remove a journal account, click the **Delete** ( ) icon, and confirm you want to remove the account.

How to Disable Throttling in Microsoft Exchange Server 2007 and 2010

> This article refers to the Barracuda Message Archiver release 3.5 or higher, and Microsoft® Exchange Server 2007 and 2010. If you are using Microsoft Exchange Server 2013, refer to How to Disable Throttling in Microsoft Exchange Server 2013.

Microsoft Exchange Server 2007 and 2010 message throttling policies set bandwidth limits and restrict the number of processed messages. In order to disable throttling, you must create an appropriate policy and assign it to the service account as documented in the Microsoft TechNet article Set Throttling Policy.

> Following is a guideline; adjust as necessary for your environment.

Assign Permissions

> **Service Account**
> For more information on creating a Service account, refer to Creating an Email Service Account for Microsoft Exchange Server 2007, 2010, and 2013.

Use the following steps to assign the Microsoft Exchange Server service account to the Application Impersonation Management role:

1. Log in to the Exchange Server as the administrator.
2. From the **Start** menu, go to **Start > Programs > Microsoft Exchange Server 2010 > Exchange Management Shell**.
3. At the command prompt, type the following command:
   ```
   New-ManagementRoleAssignment -Name:exchangeImpersonation
   -Role:ApplicationImpersonation -User:serviceAccount
   ```

Create and Assign Throttling Policy

Use the following steps to create and assign a new throttling policy, replacing *PolicyName* with the new policy name, and replacing *PolicyAdmin* with the Exchange Server 2010 service account:

1. Log in to the Exchange Server as the administrator.
2. From the **Start** menu, go to **Start > Programs > Microsoft Exchange Server 2010 > Exchange Management Shell**.
3. At the command prompt, type the following command:
   `New-ThrottlingPolicy` *`PolicyName`*
4. Press **Enter**. At the command prompt, type the following command:
   ```
   Set-ThrottlingPolicy PolicyName -RCAMaxConcurrency $null -RCAPercentTimeInAD $null
   -RCAPercentTimeInCAS $null -RCAPercentTimeInMailboxRPC $null -EWSMaxConcurrency $null
   -EWSPercentTimeInAD $null -EWSPercentTimeInCAS $null -EWSPercentTimeInMailboxRPC $null
   -EWSMaxSubscriptions $null -EWSFastSearchTimeoutInSeconds $null -EWSFindCountLimit $null
   ```
5. Press **Enter**. At the command prompt, type the following command:
   `Set-Mailbox "`*`PolicyAdmin`*`" -ThrottlingPolicy` *`PolicyName`*
6. Press **Enter**.

Microsoft Exchange Server 2003 Deployment

Recommended Method

- Microsoft Exchange Server 2003 Deployment Template
- Understanding Microsoft Exchange Server 2003 Envelope Journaling
- Configuring an SMTP Journal Account for Microsoft Exchange Server 2003
- For a PDF version of this deployment, see the Document Downloads page

Alternate Method

- Configuring an IMAP4 or POP3 Journal Account for Microsoft Exchange Server 2003

See Also

- Microsoft Exchange Server 2003, 2007, and 2010 Integration describes how to automatic import, stub, and synchronize Microsoft Exchange Server folder data.

Microsoft Exchange Server 2003 Deployment Template

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher, and a Microsoft® Exchange Server 2003 Standard Edition version using SMTP (push) journaling.

This template is a based on a *typical onsite deployment* of the Barracuda Message Archiver with Microsoft Exchange Server 2003 Standard Edition. This template describes the initial Barracuda Message Archiver setup for this deployment.

In this article:

- Implementation Prerequisites
- Physical Installation and Console Configuration
- Firewall Ports
- Activation
- Basic and Administration Setup
- Enable Journaling
- Enable SMTP Forwarding on the Barracuda Message Archiver
- Email Service Account Creation
- Configure Exchange Integration Operations

Related Articles

- Message Archiving Concepts
- Message Import, Stubbing & Configuration
- Search Options & Configuration

Additional Resource

- Troubleshooting message journaling in Exchange Server 2003

Stubbing and Microsoft Exchange Import
For stubbing and Microsoft Exchange imports initiated via the Barracuda Message Archiver web interface, there is a 100MB limit on file import.

Configuration Guidelines
This article is intended as a configuration *guideline*; your deployment will be specific to your environment. Any administrative changes should be reviewed with your IT team before proceeding.

If you are migrating to a newer version of Exchange Server, refer to Barracuda Message Archiver and Microsoft Exchange Server Migration .

Implementation Prerequisites

You will need configuration Access to the Exchange environment, and the ability to make firewall changes, if deemed necessary.

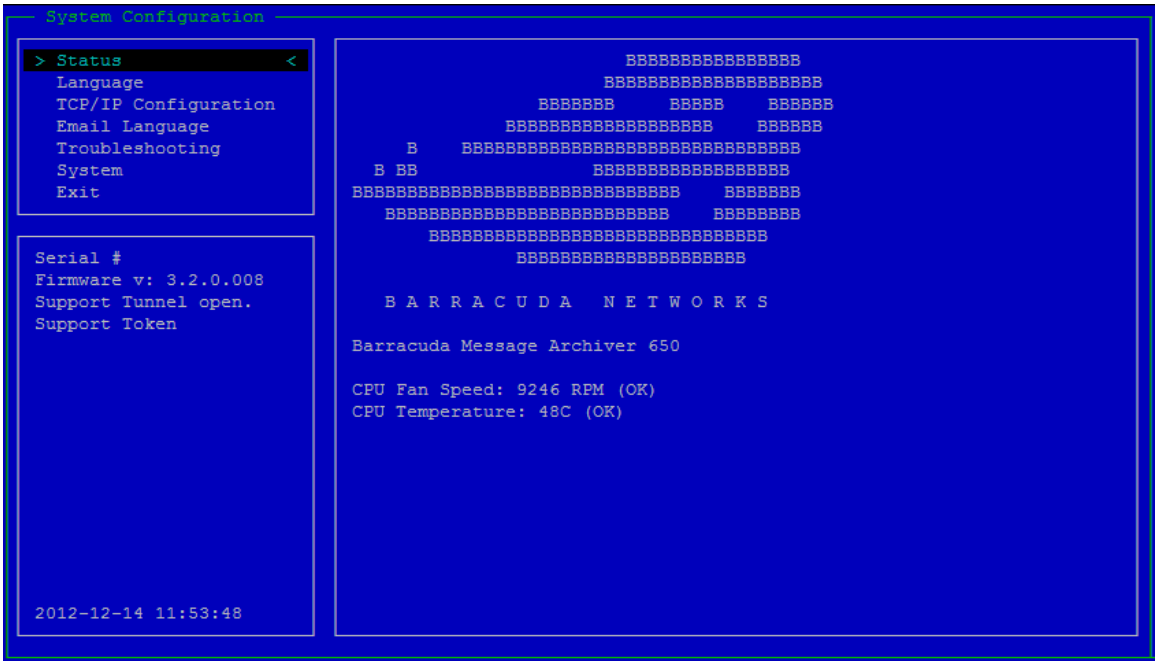
To use push journaling, you must create a *dedicated* mailbox store.

> Microsoft recommends placing the Exchange Mailbox Store containing the journaling mailbox on a drive that does not hold user mailboxes. For more information, see the Microsoft Support article Troubleshooting message journaling in Exchange Server 2003 and in Exchange 2000 Server.

Physical Installation and Console Configuration

Physically install the Barracuda Message Archiver using the following steps:

1. Fasten the Barracuda Message Archiver to a 19-inch rack or place it in a stable location.
2. Connect an Ethernet cable from the network switch to the Ethernet port on the back of the Barracuda Message Archiver.
3. Connect a standard VGA monitor, PS2 keyboard, and an AC power cord to the Barracuda Message Archiver. Press the **Power** button on the front panel to turn the unit on.
4. Log into the console using **admin/admin**, and configure the **IP Address, Subnet Mask, Default Gateway, Primary DNS Server**, and **Secondary DNS Server** as appropriate for your network:



Firewall Ports

If the Barracuda Message Archiver is located behind a corporate firewall, open the following ports on the firewall to ensure proper operation:

Port	Direction	TCP	UDP	Usage
22	Out	Yes	No	Remote diagnostics and service *recommended* (1)
25	Out	Yes	No	Email and bounces (25 inbound may be necessary for some deployments)
53	Out	Yes	Yes	Domain Name Service (DNS) *recommended*

80 and 443	Out	Yes	No	Virus, Policy, and Document Definition updates
123	In/Out	No	Yes	Network Time Protocol (NTP) *recommended*
(1) Access via Port 22 is required only if Barracuda Networks Technical Support is requested.				

Activation

Complete the following steps to activate and configure the Barracuda Message Archiver:

1. In the browser address bar enter **http://** followed by the Barracuda Message Archiver IP address, followed by the default web interface HTTP Port **:8000**. For example:
   `http://192.168.200.200:8000`
2. Use the login credentials **admin/admin**
3. In the web interface, you will see the activation warning:

Error: Activation has not been completed. Please activate your Barracuda Message Archiver to enable functionality. (Click here to activate)

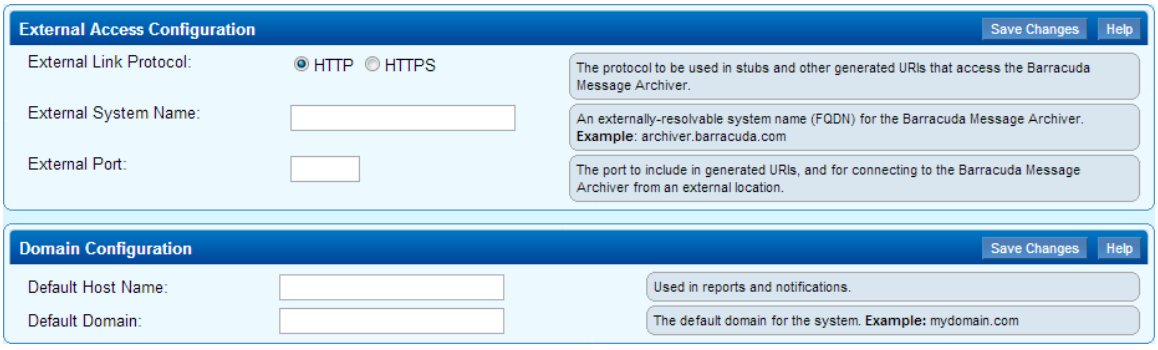
4. Click on the link to open the **Product Activation** page, fill in the required fields, and click **Activate**. The activation process may take up to 15 minutes. A confirmation page displays the terms of your subscription, and the subscription status displays as Activated on the **BASIC > Status** page.
5. Go to **ADVANCED > Firmware Update** page, and download and apply the latest General Release; allow the system to reboot.

Basic and Administration Setup

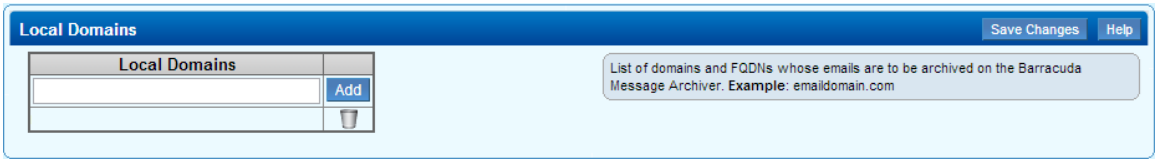
1. Once the system reboots, log back into the web interface.
2. Go to the **BASIC > IP Configuration** tab, and enter the configuration settings including external access configuration and default hostname. In the **External Access Configuration** and **Domain Configuration** sections, complete the following steps; do *not* click **Save Changes** until you complete both *of the following bullet points*:
   - In the **External Access Configuration** section, specify the protocol, and enter the FQDN of your Barracuda Message Archiver for example, archiver.mydomain.com, and enter the port number.

> **External Access**
> To allow *external* access to the Barracuda Message Archiver, you must enter an *External System Name* and *Port* that are resolvable from outside your organization's internal network. These values are used for stubbing operations and Barracuda Message Archiver Add-In integration.

   - In the **Domain Configuration** section, enter the domains. Note that depending on your environment these may match the FQDN or may be internally registered names:


External Access Configuration
Save Changes
Help
External Link Protocol:
HTTP
HTTPS
The protocol to be used in stubs and other generated URIs that access the Barracuda Message Archiver.
External System Name:
An externally-resolvable system name (FQDN) for the Barracuda Message Archiver. Example: archiver.barracuda.com
External Port:
The port to include in generated URIs, and for connecting to the Barracuda Message Archiver from an external location.
Domain Configuration
Save Changes
Help
Default Host Name:
Used in reports and notifications.
Default Domain:
The default domain for the system. Example: mydomain.com

3. Click **Save Changes** once you have completed *both of the preceding bullet points*.
4. The **Local Domains** section should include all domains from which to accept mail for archive. This identifies internal and external email:


Local Domains
Save Changes
Help
Local Domains
Add
List of domains and FQDNs whose emails are to be archived on the Barracuda Message Archiver. Example: emaildomain.com

Define external access configuration to determine how to integrate with other Barracuda Message Archiver tools and Add-Ins. Define internal or external DNS names depending on how you want to deploy Add-Ins, for example, message stubbing.

5. Go the **BASIC > Administration** page, and configure access, management, and default display settings. For more information, refer to the article How to Configure Administrative Settings.

Enable Journaling

To set up journaling, complete all of the steps described in the article Configuring an SMTP Journal Account for Microsoft Exchange 2003.

Enable SMTP Forwarding on the Barracuda Message Archiver

On the Barracuda Message Archiver, go to the **MAIL SOURCES > SMTP/IM** page, and use the following steps to enable SMTP forwarding:

1. In the **SMTP/IM Forwarding Settings** section, set **SMTP/IM Forwarding** to **Yes**.
2. In the **Trusted SMTP Servers** section, enter the IP address of each Microsoft Exchange 2003 Server that is to journal directly to the Barracuda Message Archiver.

Email Service Account Creation

To import historical data from your Exchange Server, you can create an email service account. For more information, refer to the article Creating an Email Service Account for Microsoft Exchange Server 2003.

Configure Exchange Integration Operations

1. Log in to the Barracuda Message Archiver web interface, and go to the **MAIL SOURCES > Exchange Integration** page.
2. Click **Start New Action** to define the Exchange actions to execute:
   - **Email Import** – Import all email from your Exchange Server into the Barracuda Message Archiver that meets the specified criteria. Select to import email for all users, or specify import by user name, email address, last name, public folders, or a distribution list.
   - **Non-Email Sync** – Import only non-email Exchange items into the Barracuda Message Archiver from specified accounts including Appointments, Contacts, Tasks, and Notes.
   - **Email Stubbing** – Locate messages on your Exchange Server that meet the specified criteria, copy the specified parts (just attachments, or the entire message with or without attachments) onto the Barracuda Message Archiver, and modify those messages on your Exchange Server so that appropriate parts of the messages are replaced with a stub (a link to where the actual contents reside on the Barracuda Message Archiver).
   - **Folder Sync** – Import into the Barracuda Message Archiver the complete folder structure of the selected users' Mailboxes. This action imports the selected users' custom folders and subfolders.
3. Use the workflow to set up the Exchange action.

For a comprehensive description of each Exchange Action, go to the **MAIL SOURCES > Exchange Integration** page in the web interface and click **Help**.

Next Step: Proceed to the article **Configuring an SMTP Journal Account for Microsoft Exchange 2003** to complete your deployment setup.

Understanding Microsoft Exchange 2003 Envelope Journaling

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher, and a Microsoft® Exchange Server 2003.

Organizations using Microsoft Exchange Server 2003 can take advantage of its envelope journaling feature to send all messages, along with all recipient information, directly to the Barracuda Message Archiver ensuring complete and accurate archiving of all electronic correspondence for compliance with government regulations and corporate standards.

Stubbing and Microsoft Exchange Import
For stubbing and Microsoft Exchange imports initiated via the Barracuda Message Archiver web interface, there is a 100MB limit on file import.

Important

If you are migrating to a newer version of Exchange Server, refer to Barracuda Message Archiver and Microsoft Exchange Server Migration.

How it Works

In Microsoft Exchange 2003, journaling is enabled at the mailbox store level. Configuring envelope journaling allows messages sent to the journaling mailbox to retain complete recipient information including 'bcc' recipients. If envelope journal headers are available, the Barracuda Message Archiver uses these headers to determine:

- Actual recipients
- End-user archived message access permissions

Important - Journaling Options
Journaled mail can be sent to the Message Archiver via SMTP or "push journaling", or journaled mail can remain in the journal mailbox and retrieved via POP3 or IMAP or "pull" method of journaling. If you are unable to create an additional mail store, instead of using SMTP to push mail, you can use the pull method to journal mail content using POP3 or IMAP:

- If you are running *Microsoft Exchange Server 2003 Enterprise Edition* and you want to use Push Journaling, see Configuring an SMTP Journal Account for Microsoft Exchange 2003.
- If you are running *Microsoft Exchange Server 2003 Standard Edition*, or if you want to use Pull Journaling, see Configuring an IMAP or POP3 Journal Account for Microsoft Exchange 2003.

Best Practice
To use push journaling, you must create a *dedicated* mailbox store for the envelope journaling mailbox, otherwise mail arriving in the mailbox results in unwanted mail loops.

Microsoft recommends placing the Exchange Mailbox Store containing the journaling mailbox on a drive that *does not hold user mailboxes.* For more information, see the Microsoft article Troubleshooting message journaling in Exchange Server 2003 and in Exchange 2000 Server.

To ensure messages display properly in all standard mail clients, save messages in Multipurpose Internet Mail Extensions (MIME) multipart format.

It is possible to send messages and other Exchange data directly from the mailbox database to an archive over SMTP using Microsoft Outlook server-side rules or Active Directory Users and Computers (ADUC) Exchange Properties. However, messages sent based on these settings *do not* include envelope information.

Important
Exchange cannot fully journal the following:

- **Posts to public folders** - Journaling cannot be enabled on public folder stores.
- **Expansion of external distribution lists** - While actual message content sent to or from internal and external distribution lists can be journaled, only an internal distribution list can be fully expanded and included in the envelope journaling data. Membership information for a distribution list that is external to your Exchange organization cannot be expanded and therefore cannot be included in the envelope information even if individual members on the list are in your Exchange server.

Configuring an SMTP Journal Account for Microsoft Exchange 2003

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher, and a Microsoft® Exchange Server 2003.

In this article:

- Before Getting Started
- Configuration
- Step 1. Create a Mailbox Store for the Journaling Mailbox
- Step 2. Create Remote Domain
- Step 3. Set Up Message Routing for Journal Contact

- Step 4. Create a Journal Account Mailbox
- Step 5. Create a Custom SMTP Recipient
- Step 6. Hide Mail Contact in Exchange Global Address List, Modify SMTP Addresses, and Enable Server-Side Mailbox Forwarding
- Step 7. Modify Journal Mail Contact
- Step 8. Enable Envelope Journaling on Mail Storage
- Step 9. Configure Exchange Mailbox Management
- Step 10. Verify Journaling is Functioning as Expected

Related Articles

- Compliance
- Set Up Email Journaling
- Exchange 2003 Envelope Journaling
- Message Import, Stubbing & Configuration
- Understanding SMTP Forwarding and Trusted Servers

Additional Resource

- Troubleshooting message journaling in Exchange Server 2003 and in Exchange 2000 Server

Server Edition
This article applies to Microsoft Exchange Server 2003 Enterprise Edition; if you are using Microsoft Exchange Server 2003 Standard Edition, contact Barracuda Networks Technical Support for details on configuring an IMAP or POP3 Journal Account for Microsoft Exchange 2003.

If you are migrating to a newer version of Exchange Server, refer to Barracuda Message Archiver and Microsoft Exchange Server Migration.

Stubbing and Microsoft Exchange Import
For stubbing and Microsoft Exchange imports initiated via the Barracuda Message Archiver web interface, there is a 100MB limit on file import.

Before Getting Started

Read this entire section *before* proceeding with configuration.

Important - Journaling Options
Journaled mail can be sent to the Message Archiver via SMTP or "push journaling", or journaled mail can remain in the journal mailbox and retrieved via POP3/IMAP or "pull journaling". If you are *unable* to create an additional mail store, use POP3 or IMAP to "pull" mail content to the Barracuda Message Archiver, contact Barracuda Networks Technical Support.

Important
To use push journaling, you must create a *dedicated* mailbox store for the envelope journaling mailbox, otherwise mail arriving in the mailbox results in unwanted mail loops.

Microsoft recommends placing the Exchange Mailbox Store containing the journaling mailbox on a drive that *does not hold user mailboxes.* For more information, see the Microsoft Tech net article Troubleshooting message journaling in Exchange Server 2003 and in Exchange 2000 Server.

Important
Exchange cannot fully journal the following:

- **Posts to public folders** - Journaling cannot be enabled on public folder stores.
- **Expansion of external distribution lists** - While actual message content sent to or from internal and external distribution lists can be journaled, only an internal distribution list can be fully expanded and included in the envelope journaling data. Membership information for a distribution list that is external to your Exchange organization cannot be expanded and therefore cannot be included in the envelope information even if individual members on the list are in your Exchange server.

Configuration

To fully utilize envelope journaling, you must set up the following on the Microsoft Exchange Server 2003:

- Step1: Create a Mailbox Store for the Journaling Mailbox - Define a dedicated mailbox store for the envelope journaling mailbox, otherwise mail arriving in the mailbox results in unwanted mail loops.
- Step 2: Create Remote Domain - Create a new remote domain.
- Step 3: Set Up Message Routing for the Journal Contact - Define message routing to route journal contact via a dedicated SMTP connector.
- Step 4: Create a Journal Account Mailbox - Create a Journal account mailbox.
- Step 5: Create a Custom SMTP Recipient - Define an SMTP address in your Active Directory; this address serves as the delivery address for journaled messages.
- Step 6: Hide Mail Contact in Exchange Global Address List, Modify SMTP Addresses, and Enable Server-Side Mailbox Forwarding - Set up a server-side rule to forward all journaled messages to the custom SMTP recipient mailbox.
- Step 7: Modify Journal Mail Contact - Hide the Journal Mailbox from the Exchange Server address lists to maintain the mailbox store for envelope journaling only.
- Step 8: Enable Envelope Journaling on Exchange - Enable envelope journaling on Exchange to deliver messages using an envelope message containing a journal report with the original message as an attachment.
- Step 9: Configure Exchange Mailbox Management - Define an Outlook rule to automatically delete archived messages forwarded to the Barracuda Message Archiver from the local mailbox store to reduce storage "bloat".
- Step 10. Verify Journaling is Functioning as Expected - Verify your set up is complete.

Important

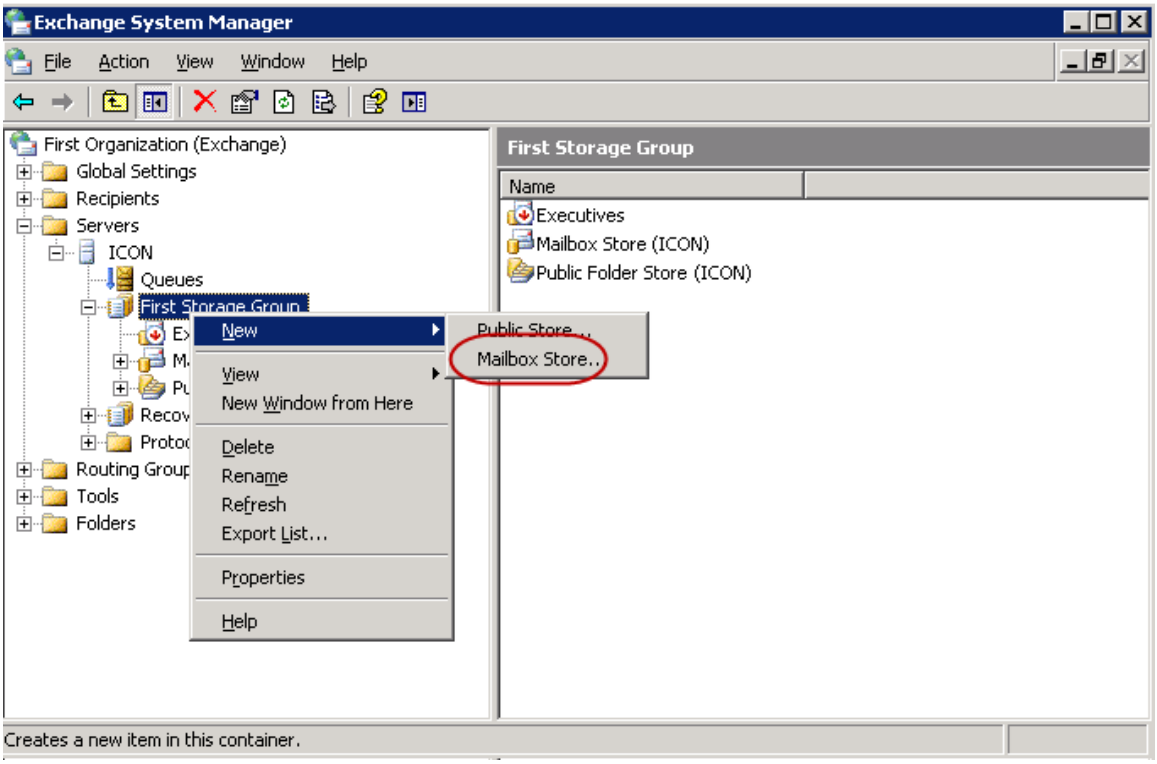
- To ensure messages display properly in all standard mail clients, save messages in Multipurpose Internet Mail Extensions (MIME) multipart format.
- It is possible to send messages and other Exchange data directly from the mailbox database to an archive over SMTP using Microsoft Outlook server-side rules or Active Directory Users and Computers (ADUC) Exchange Properties. However, messages sent based on these settings *do not* include envelope information.
- Envelope data is encapsulated with a message only *after* the message is delivered to the journaling mailbox. In other words, if a message is forwarded directly via SMTP, envelope data is not included. Therefore, it is highly recommended that ***all forwarding to the Barracuda Message Archiver occur from the journaling mailbox*** in order to retain data (including 'Bcc' recipients and a fully expanded distribution list) to ensure your archive complies with Ediscovery standards.

Step 1. Create a Mailbox Store for the Journaling Mailbox

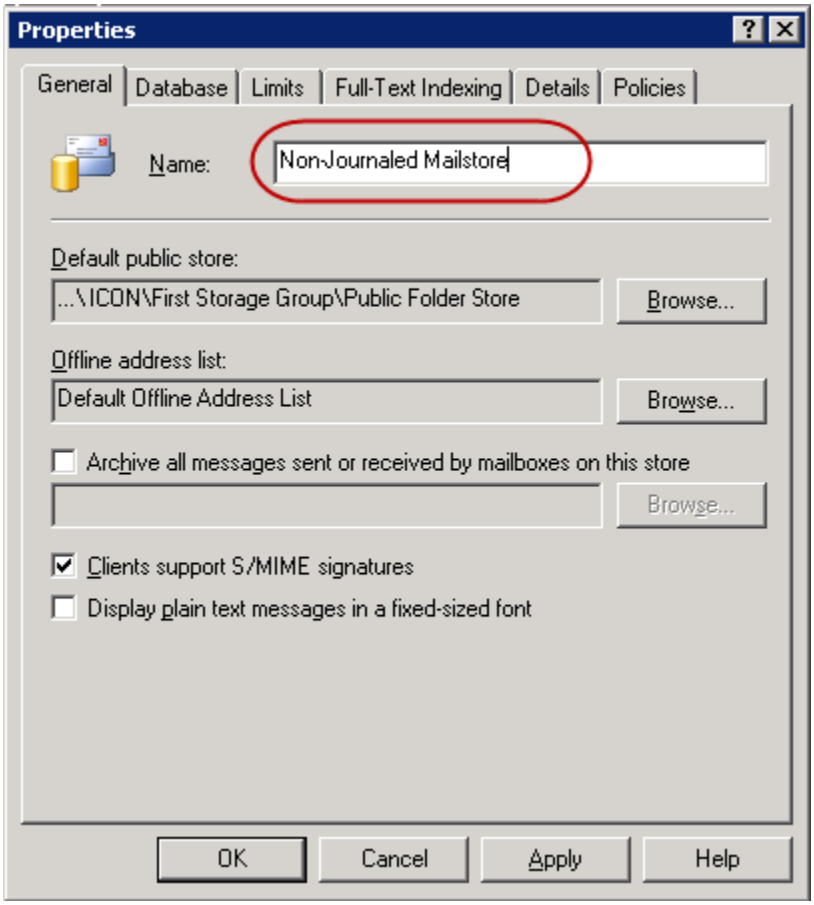
Use the following steps to add a new mailbox store on your Exchange Server.

1a. Launch the **Exchange System Manager (ESM)** console (**Programs > Microsoft Exchange > System Manager**), expand your servers, and navigate to the server in which you intend to add the mailbox store.

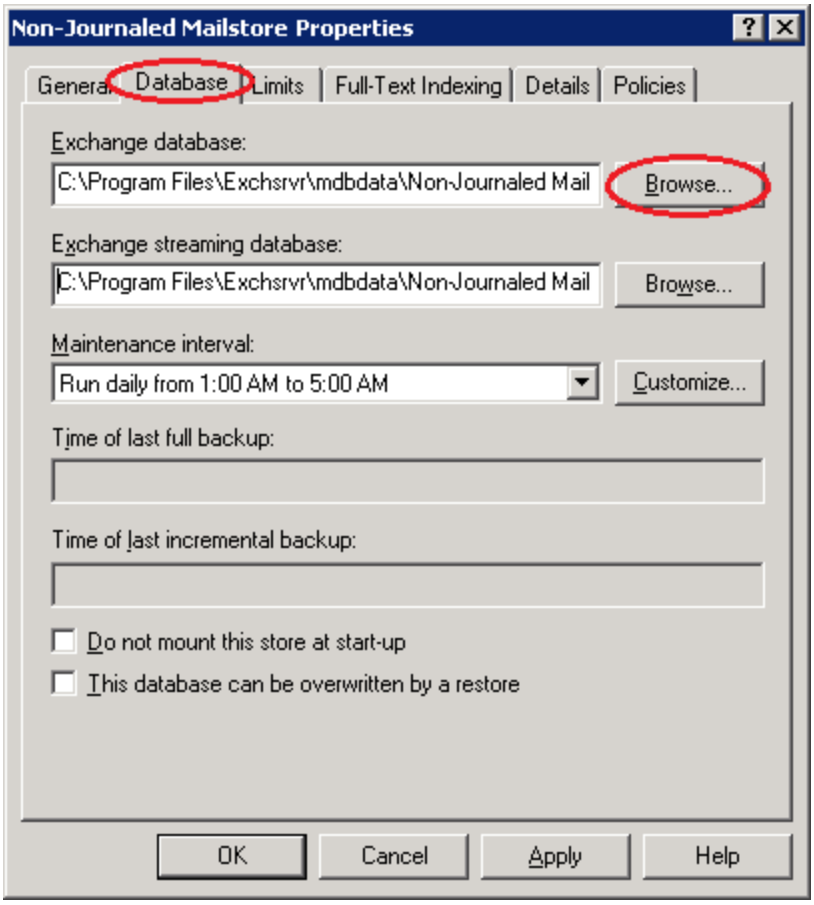
1b. Right-click **First Storage Group**, point to **New**, and click **Mailbox Store**:



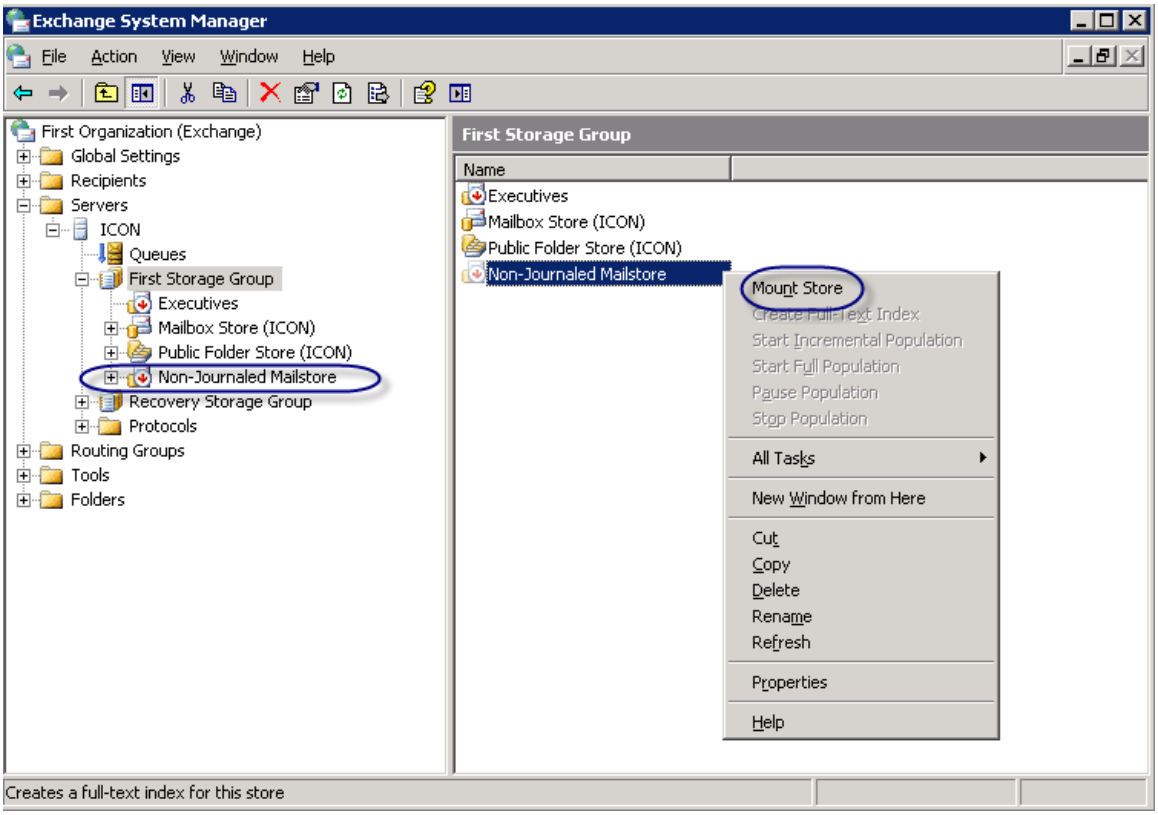
1c. In the **Properties** dialog box, click the **General** tab, and type `Non-Journaled Mailstore` in the **Name** field:



1d. Click on the **Database** tab, and click **Browse** next to the **Exchange database** field:



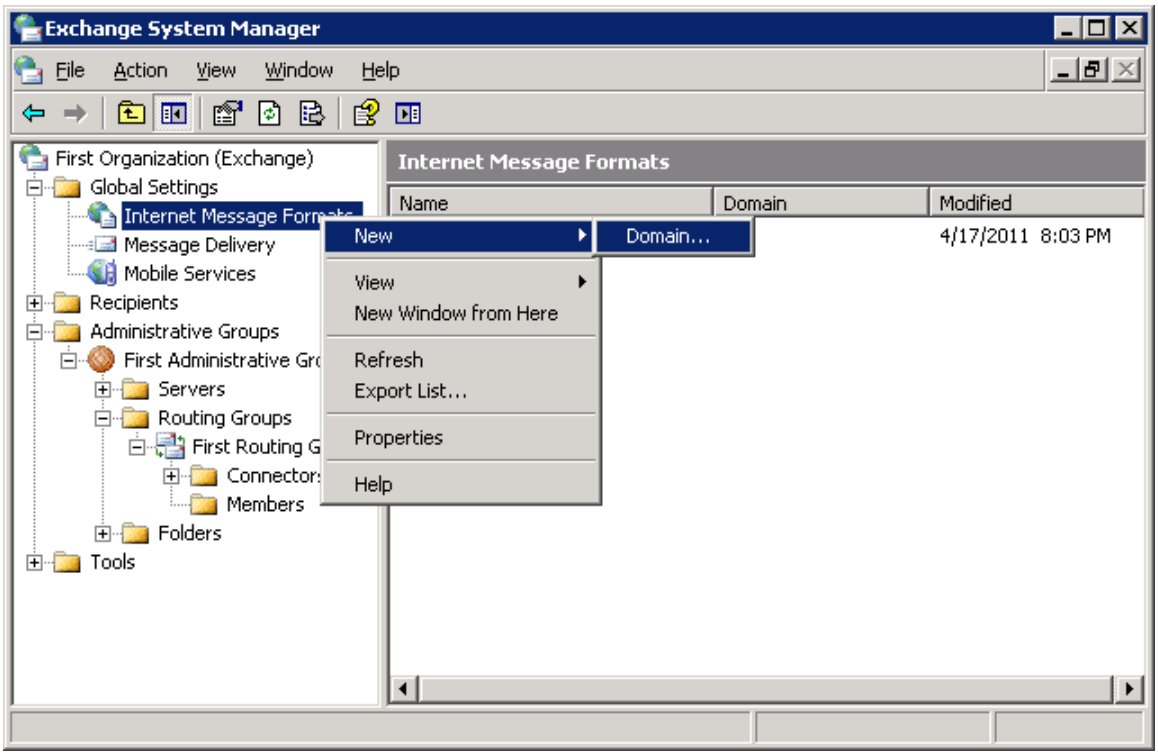
1e. Browse to and select the default database location where you want to add the mailbox store, click **Apply**, and click **OK**. The mailbox store **Non-Journaled Mailstore** displays in the **ESM**. Right-click on **Non-Journaled Mailstore**, and click **Mount Store**:



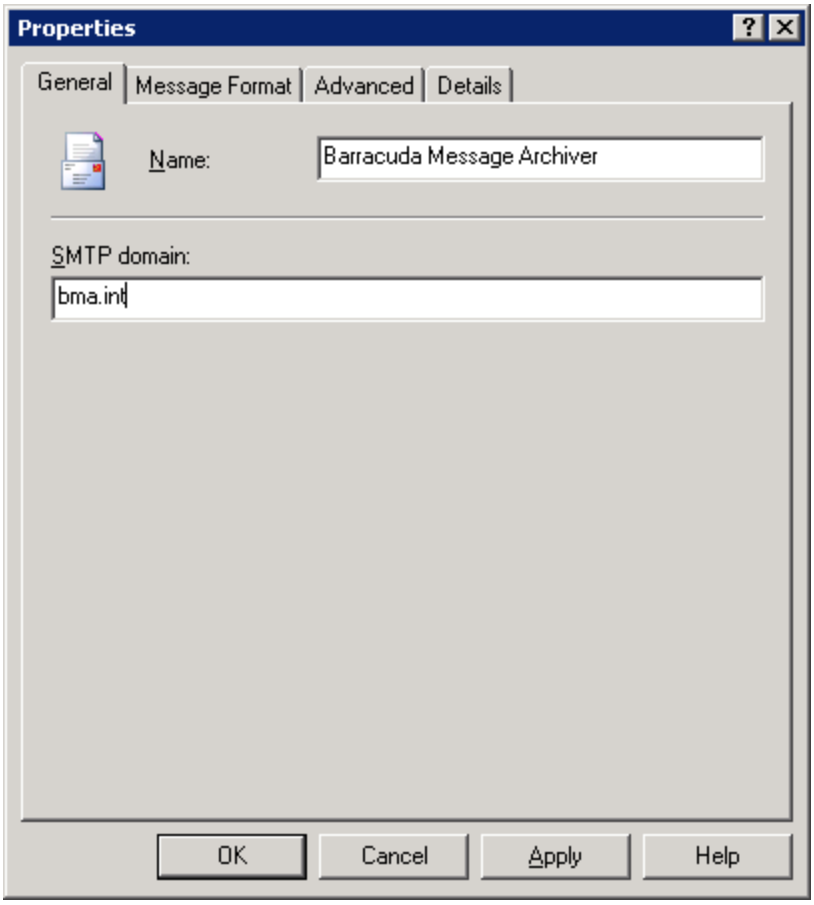
1f. Click **Allow**, and then **c**lick **OK**.

Step 2. Create Remote Domain

2a. In the **ESM** console, expand **Global Settings**, right-click **Internet Message Formats**, point to **New**, and click **Domain**:

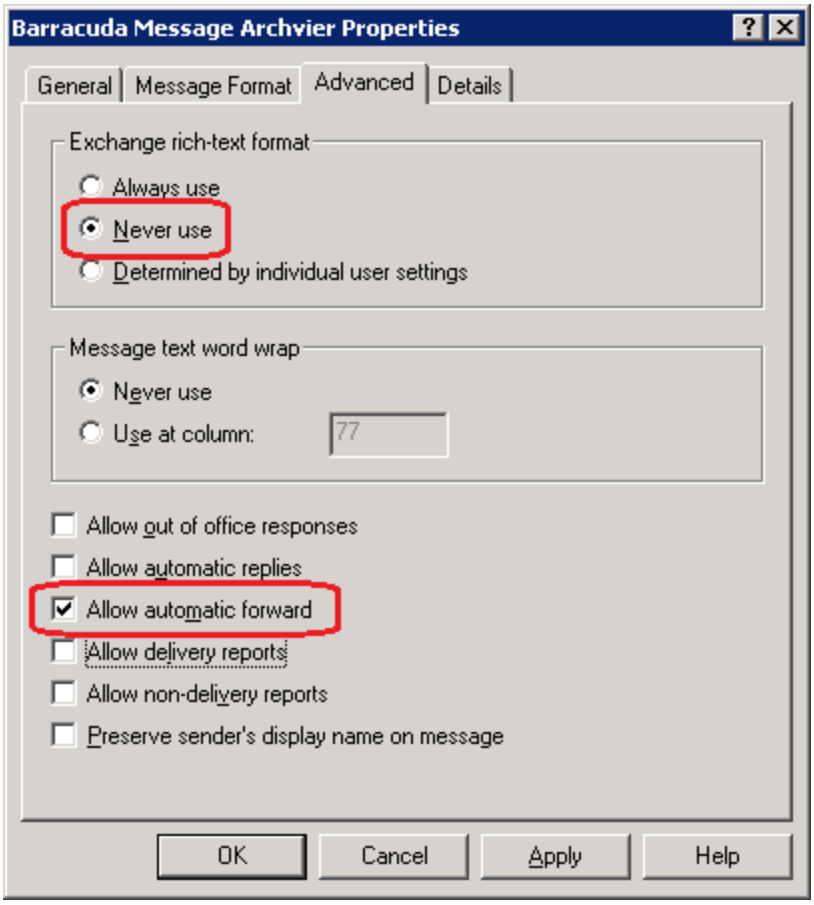


2b. In the **Properties** dialog box, enter `Barracuda Message Archiver` in the **Name** field, and in the **SMTP domain** field, type `bma.int`:



2c. Click **Apply**, click the **Advanced** tab, and in the **Exchange rich-text format** section, click **Never use**. Select **Allow automatic forward**, and deselect all other options:

Verify that only **Never use** and **Allow automatic forward** are selected in the dialog box.

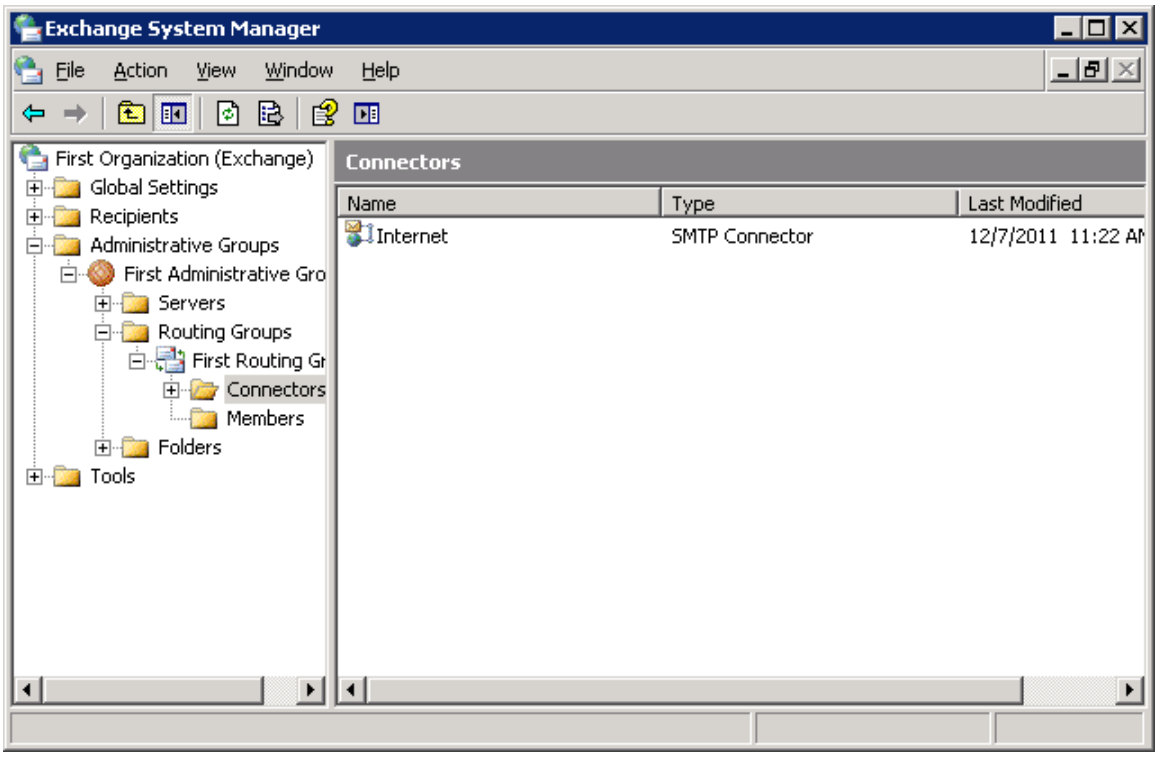


2d. Click **Apply**, and click **OK** to save your changes and close the dialog box.

Step 3. Set Up Message Routing for Journal Contact

Use the following steps to route messages specified for the Journal Contact on Microsoft Exchange Server 2003.

3a. In the **ESM**, expand **Connectors**. For example, in the default view, the **Connectors** folder is located at the top level, and in the **Administrative Group Display**, the folder is available under **Routing Groups**:

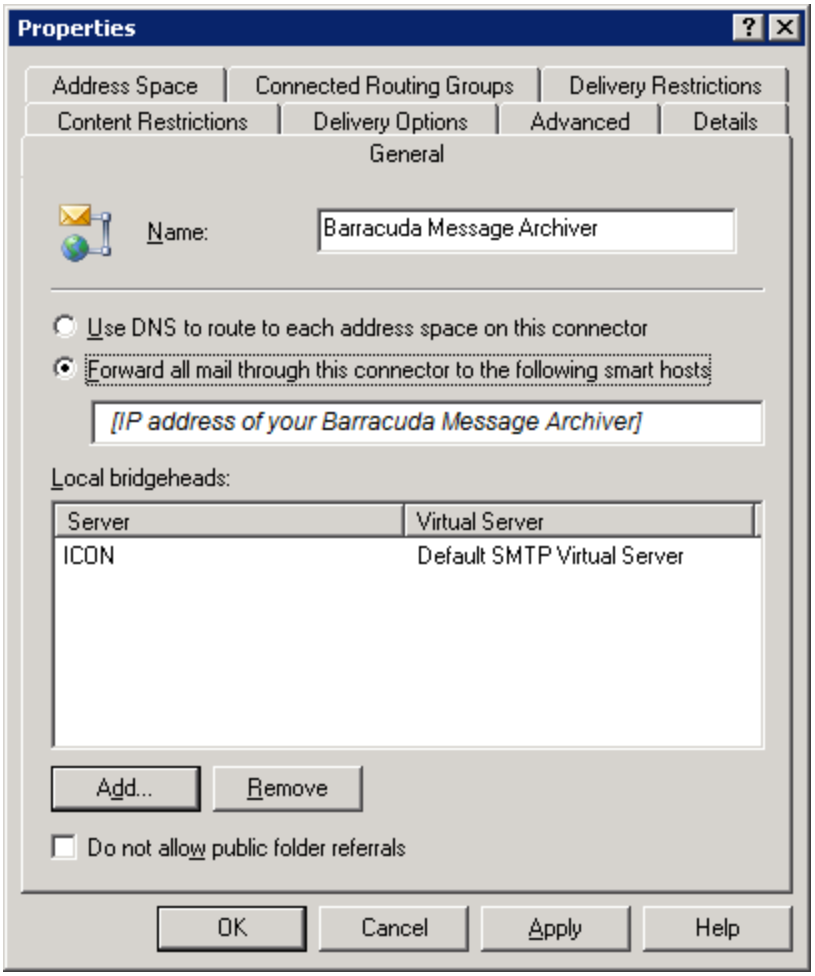


3b. Right-click **Connectors**, and click **New > SMTP Connector**. The **SMTP Connector** dialog box displays. In the **Name** field in the **General** tab, type `Barracuda Message Archiver`.

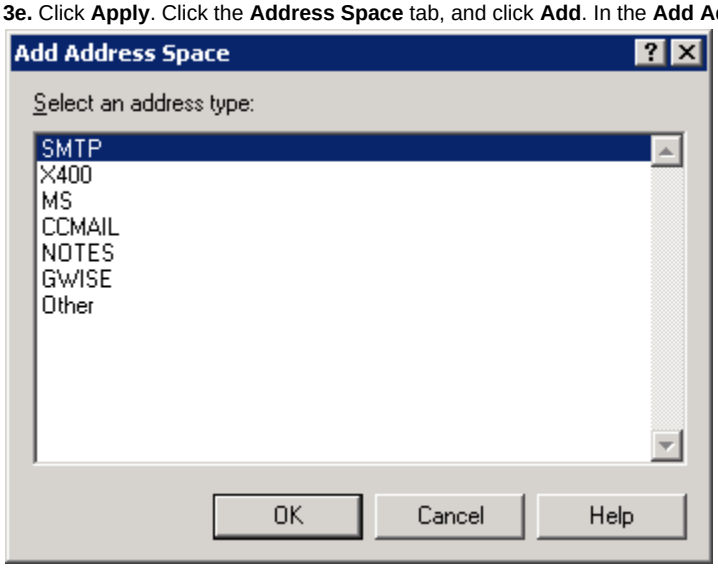
3c. Select **Forward all mail through this connector to the following smart hosts**, and enter the IP address of your Barracuda Message Archiver in the associated field enclosed in square brackets **[ ]**.

> If you do not enclose the IP address in square brackets **[ ]**, an error displays.

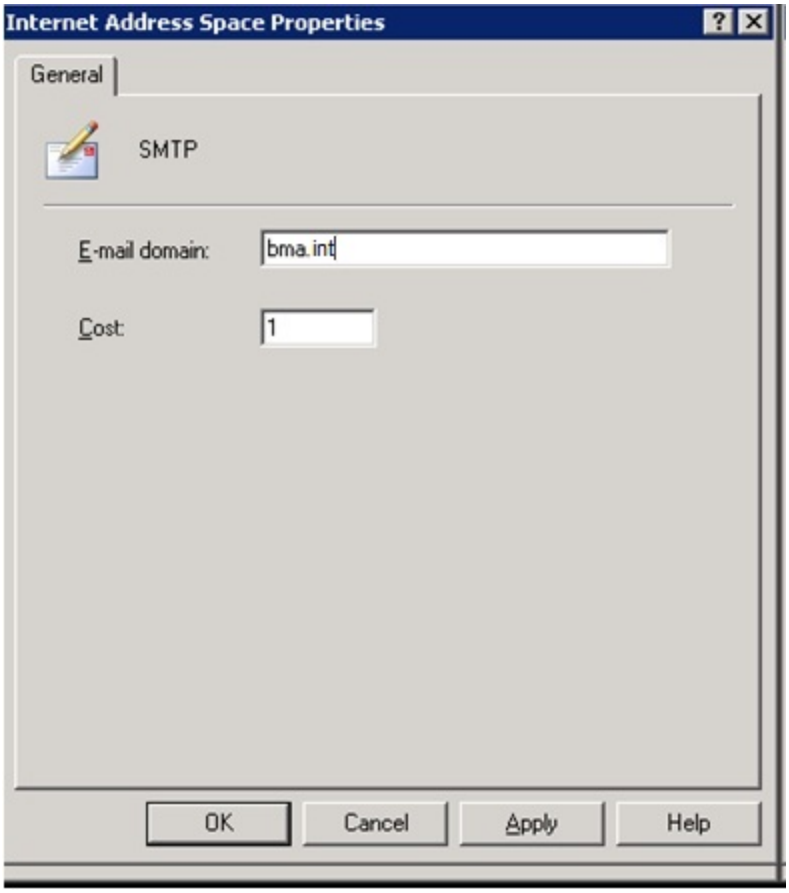
3d. Below the **Local Bridgehead** section, click **Add**. Click on your **SMTP virtual server instance**, and click **OK**; the SMTP Virtual Server is added:



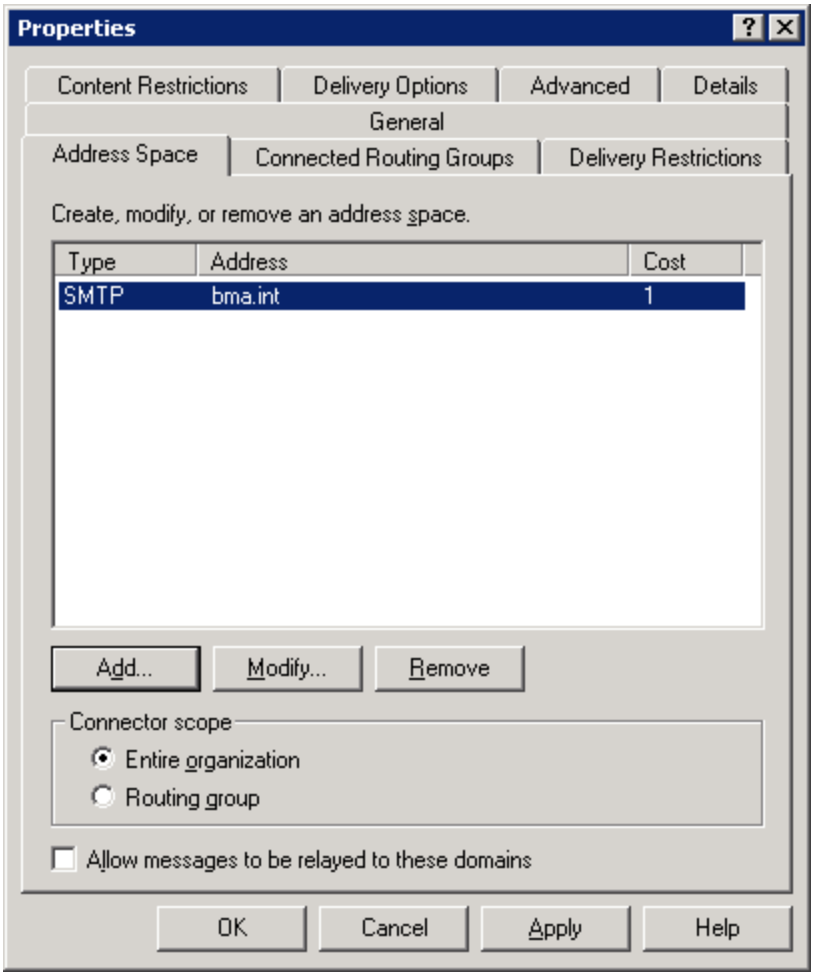
3e. Click **Apply**. Click the **Address Space** tab, and click **Add**. In the **Add Address Space** dialog box, select the address type **SMTP**:



3f. Click **OK**. The **Internet Address Space Properties** dialog box displays. Type the domain name `bma.int`:



3g. Click **Apply**, and click **OK** to close the dialog box. The new address space displays in the **Address Space** tab:



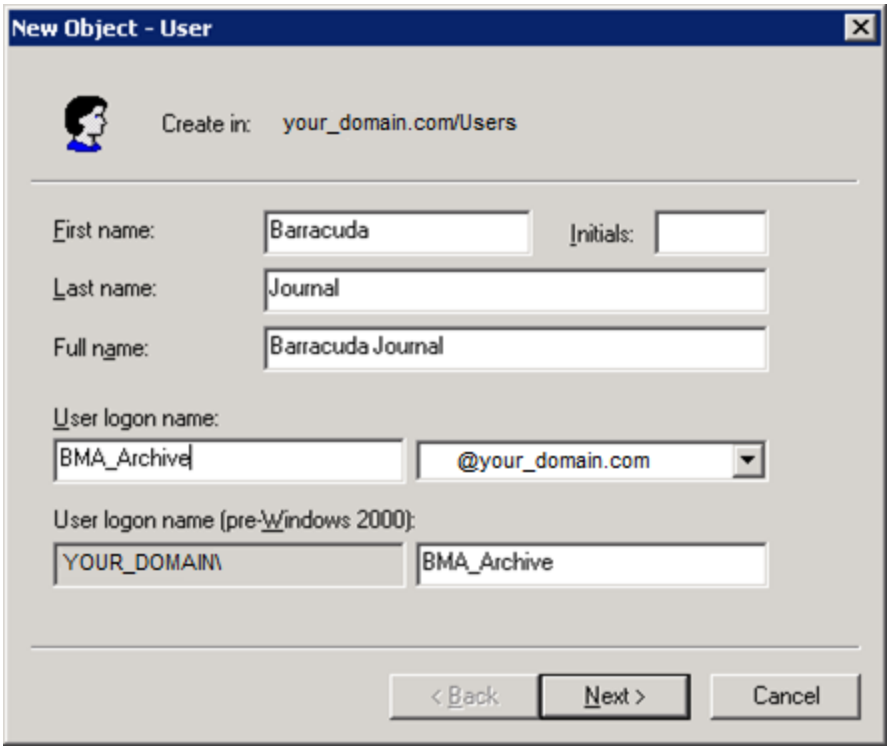
3h. Click **Apply**, and click **OK** to close the **Properties** dialog box and save your changes.

Step 4. Create a Journal Account Mailbox

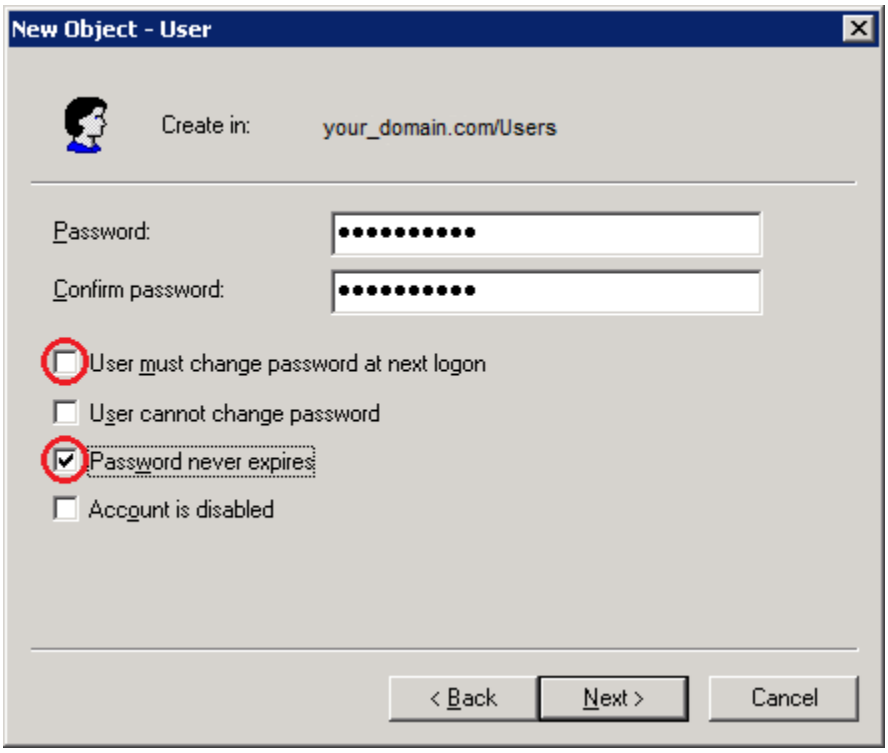
> You must create a Journal Account Mailbox for a domain or OU as described in this step on the Mailbox Store you created in **Step 1**.

4a. Launch the **Active Directory Users and Computers** console (**Programs > Administrative Tools or Programs > Microsoft Exchange**), and connect to the non-journaled Mailbox Store created in **Step 1**.

4b. Click on the domain or organization unit (OU) in which to create the Journal Account Mailbox. Right-click in the right pane, and click **New > User** to bring up the **New Object - User** dialog box. Enter the Journal User details:

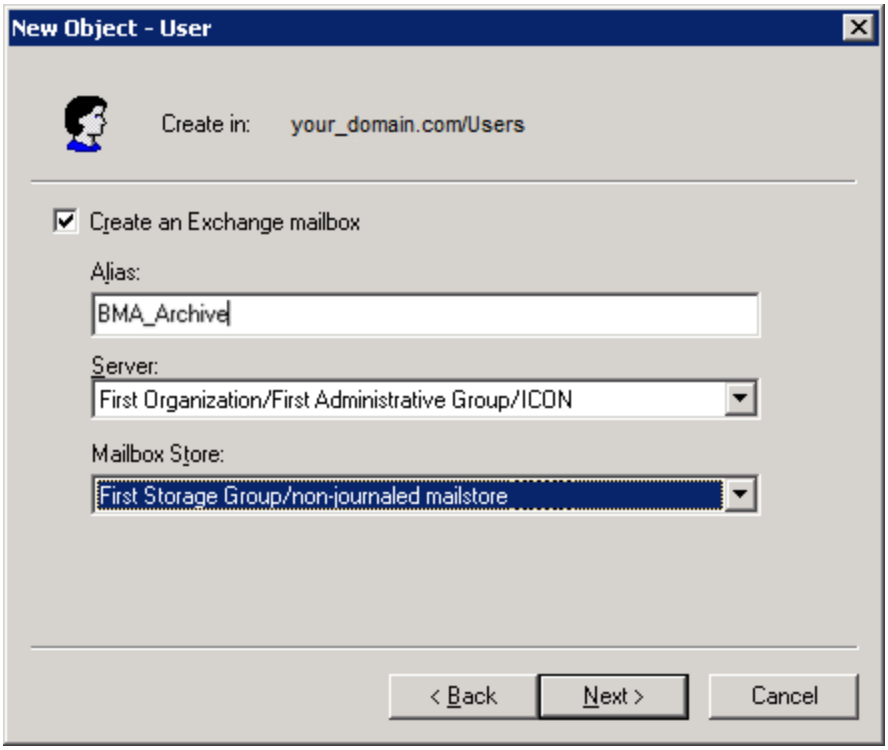


4c. Click **Next**. Enter a password in the **Password** and **Confirm password** fields, clear **User must change password at next logon**, and select **Password never expires**:



4d. Click **OK** in the warning dialog box, and then click **Next**; select **Create an Exchange mailbox**:

Verify the **Server** field points to your non-journaled mailstore location from **step 1**.



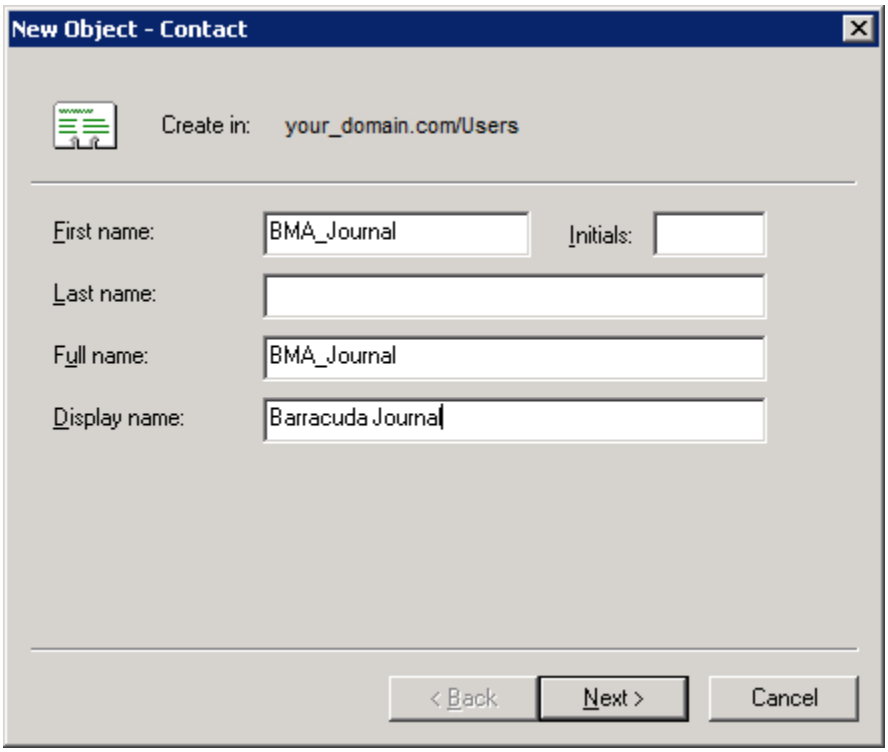
4e. Click **Next**, verify the entered information, and click **Finish** to create the User and close the dialog box.

Step 5. Create a Custom SMTP Recipient

> In this step you *disable* Microsoft MAPI Rich-Text Format (RTF).

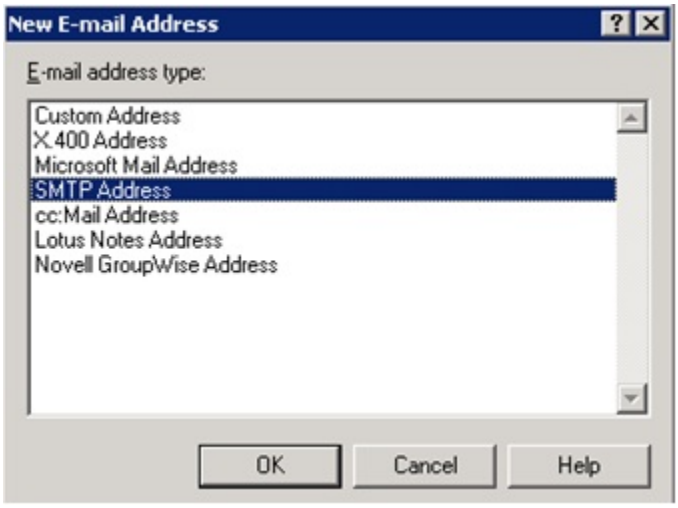
5a. In the **Active Directory Users and Computers** console, click on the domain or organization unit (OU) in which to create the custom SMTP recipient, point to **New**, and click **Contact**; the **New Object - Contact** dialog box displays.

5b. Enter the name and display name for the custom SMTP recipient:

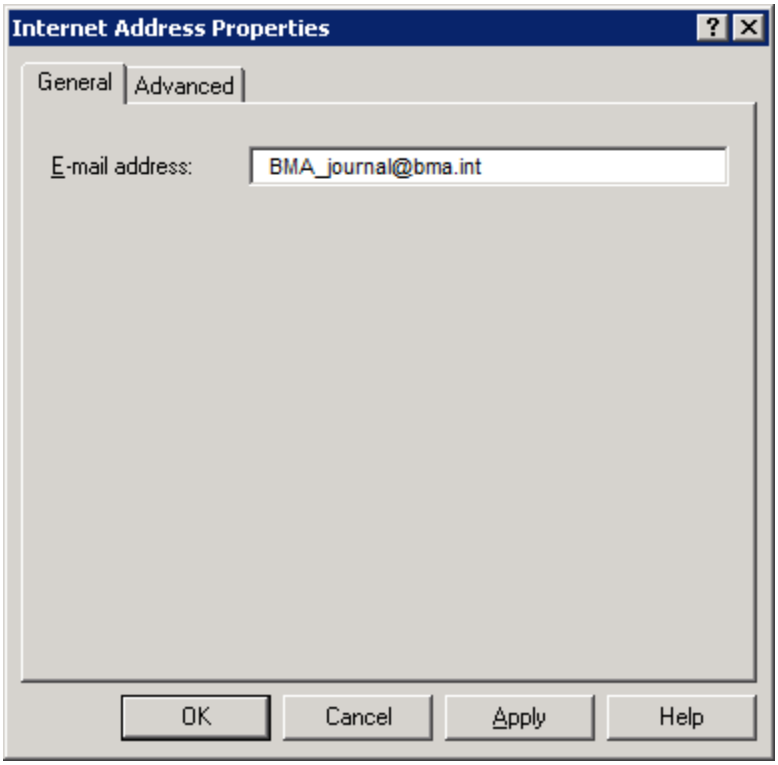


5c. Click **Next**. Select **Create an Exchange e-mail address**, enter the email alias in the **Alias** field, and click **Modify**.

5d. The **New E-mail Address** dialog box displays:



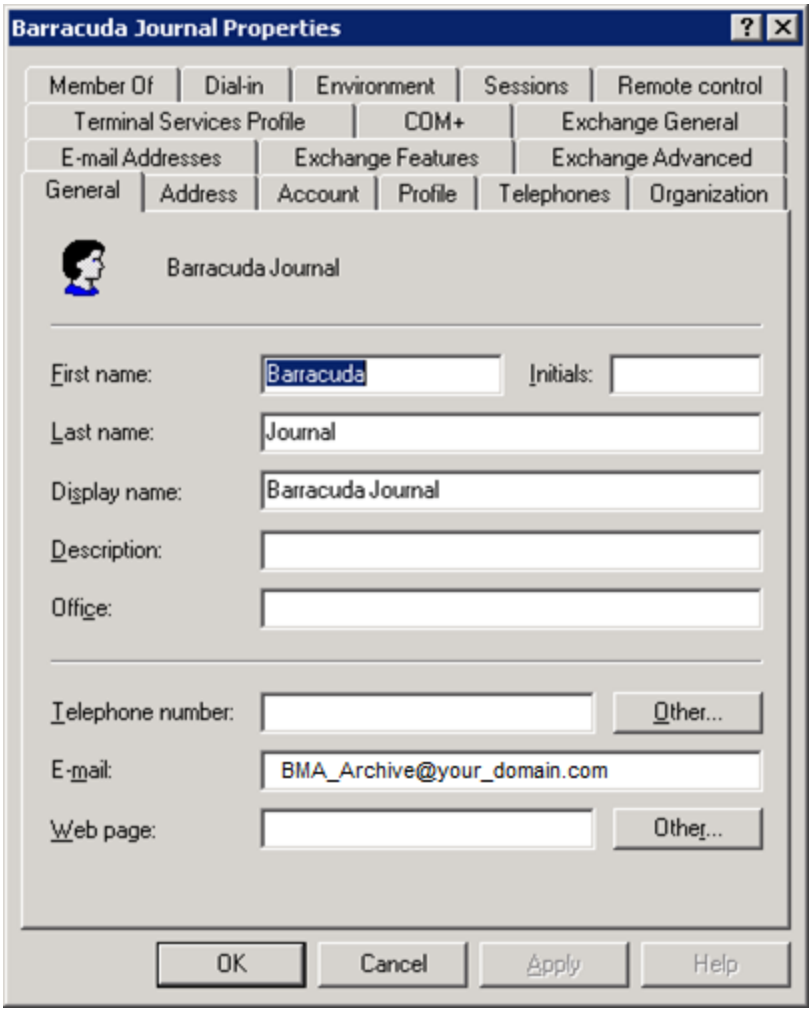
5e. Click **SMTP Address**, and click **OK**; the **Internet Address Properties** dialog box displays. In the **General** tab, enter the external email address `BMA_Journal@bma.int`:



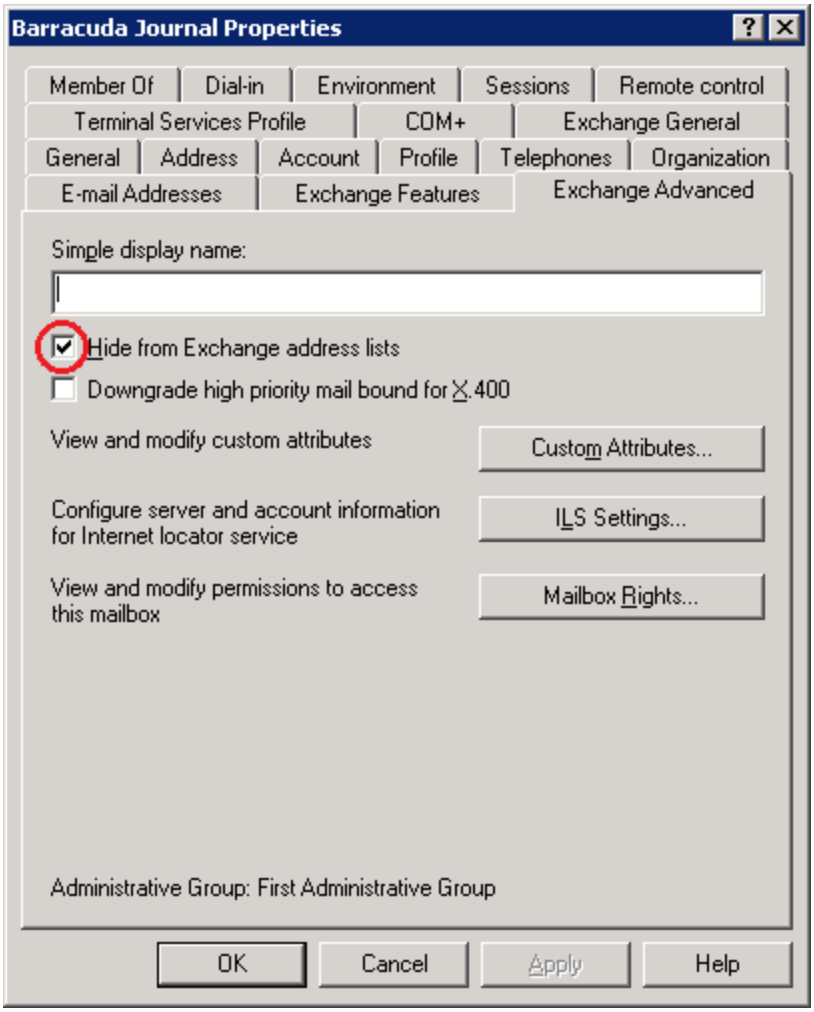
5f. Click **OK**. In the **New Object - Contact** dialog box, click **Next** and verify the entered details, click **Apply**, and click **Finish** to create the contact and close the dialog box.

Step 6. Hide Mail Contact in Exchange Global Address List, Modify SMTP Addresses, and Enable Server-Side Mailbox Forwarding

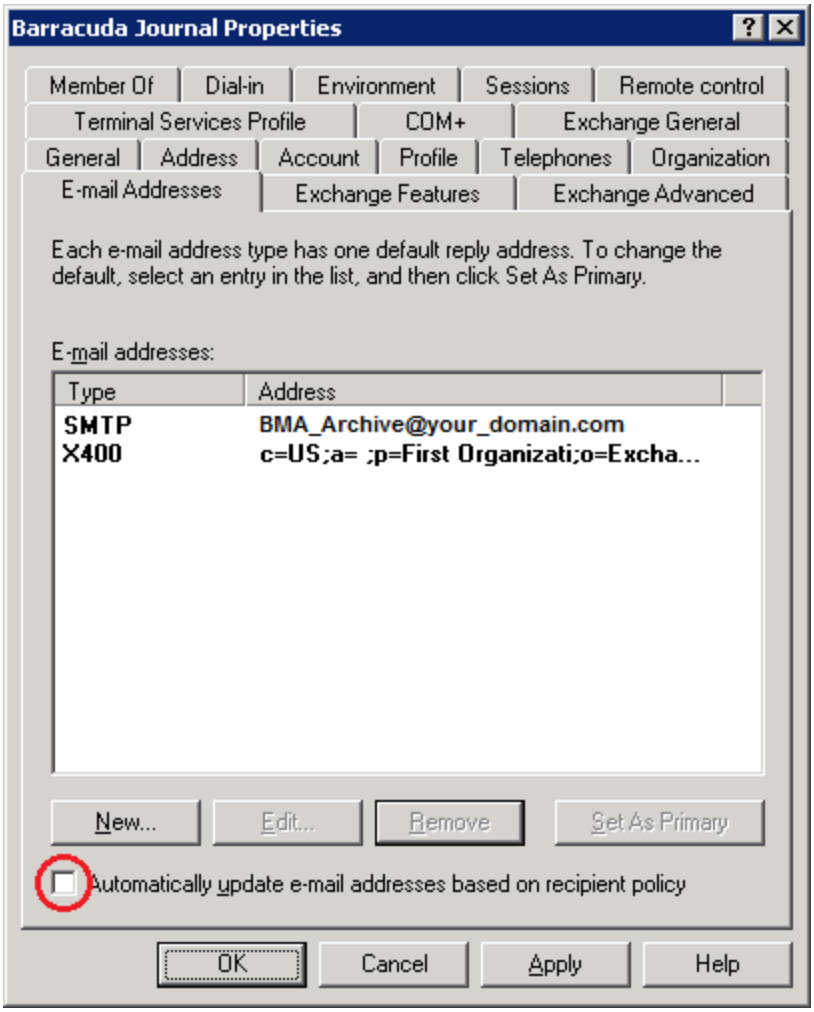
6a. In the **Active Directory Users and Computers** console, right-click on the user you created in **Step 4**, and click **Properties**:



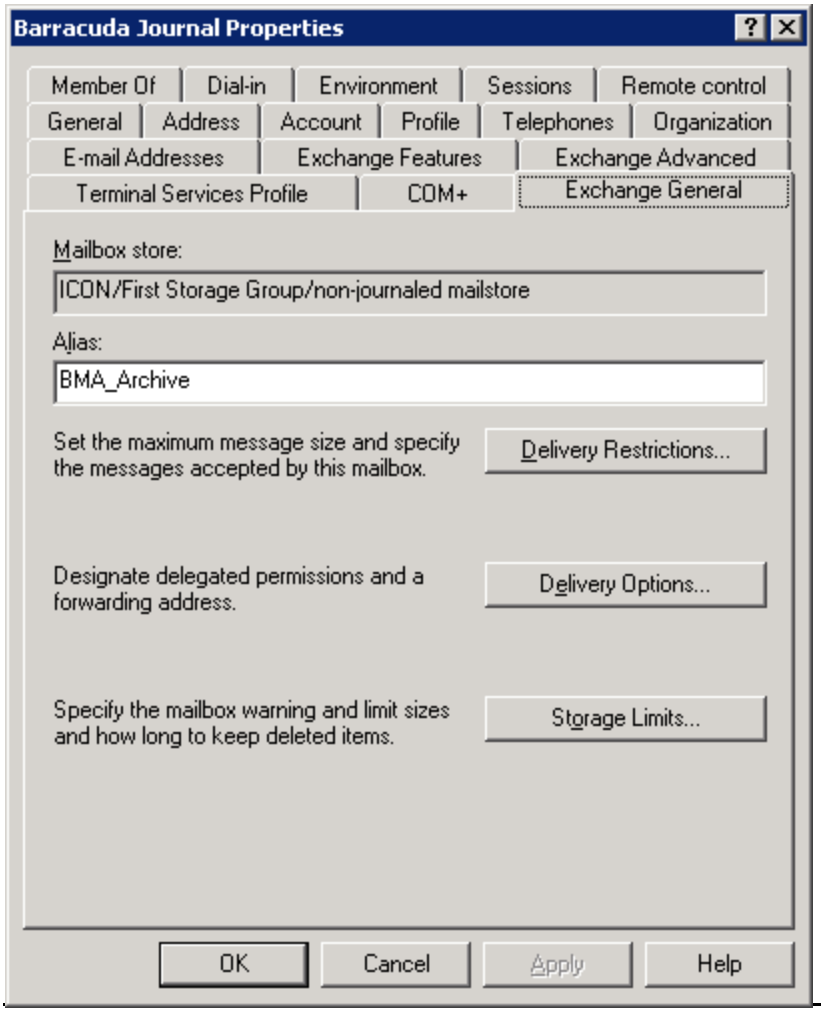
6b. Click the **Exchange Advanced** tab, and select **Hide from Exchange address lists**:



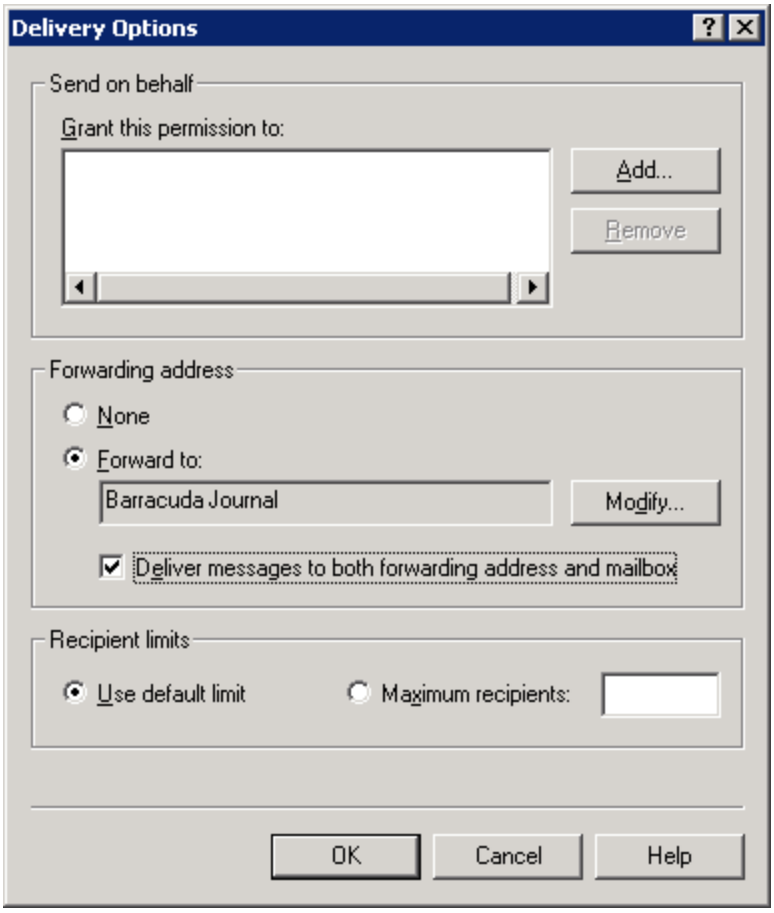
6c. Click the **E-mail Address** tab, remove all email addresses except the SMTP address, and clear **Automatically update e-mail addresses based on recipient policy**:



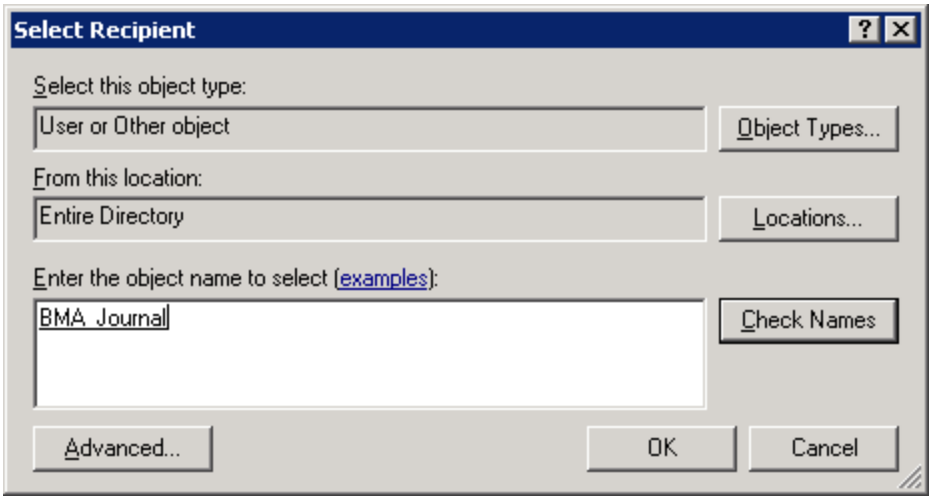
6d. Click the **Exchange General** tab:



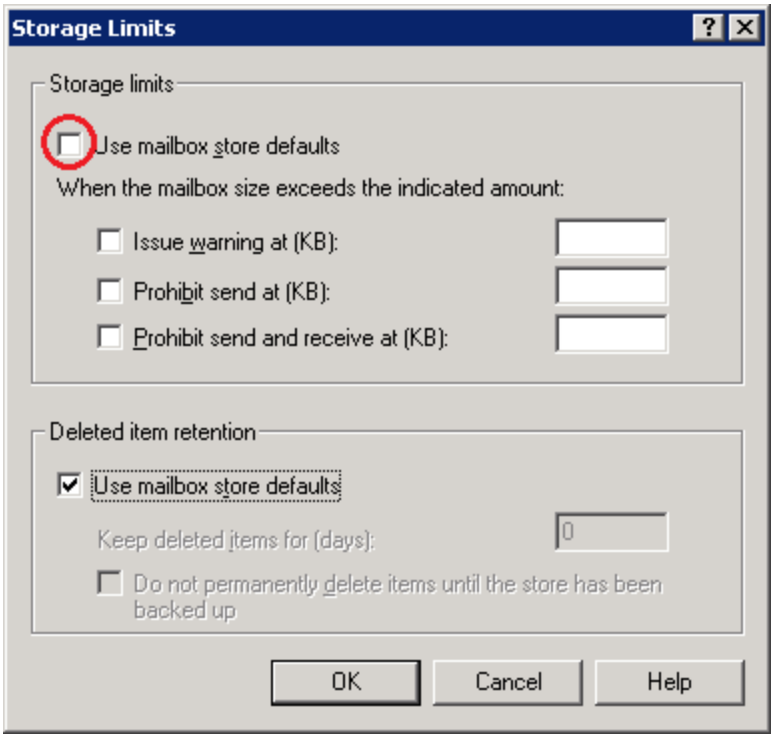
6e. Click **Delivery Options**. In the **Delivery Options** dialog box, in the **Forwarding address** section, select **Delivery Messages to both forwarding address and mailbox**, and click **Forward to**:



6f. Click **Modify to** the right of the **Forward to** field. In the **Enter the object name to select** box, type `BMA_Journal`, and click **Check Names**:



6g. Click **OK** to close the **Delivery Options** dialog box. In the **Exchange General** tab, click **Storage Limits**. In the **Storage limits** section, deselect **Use mailbox store defaults**:

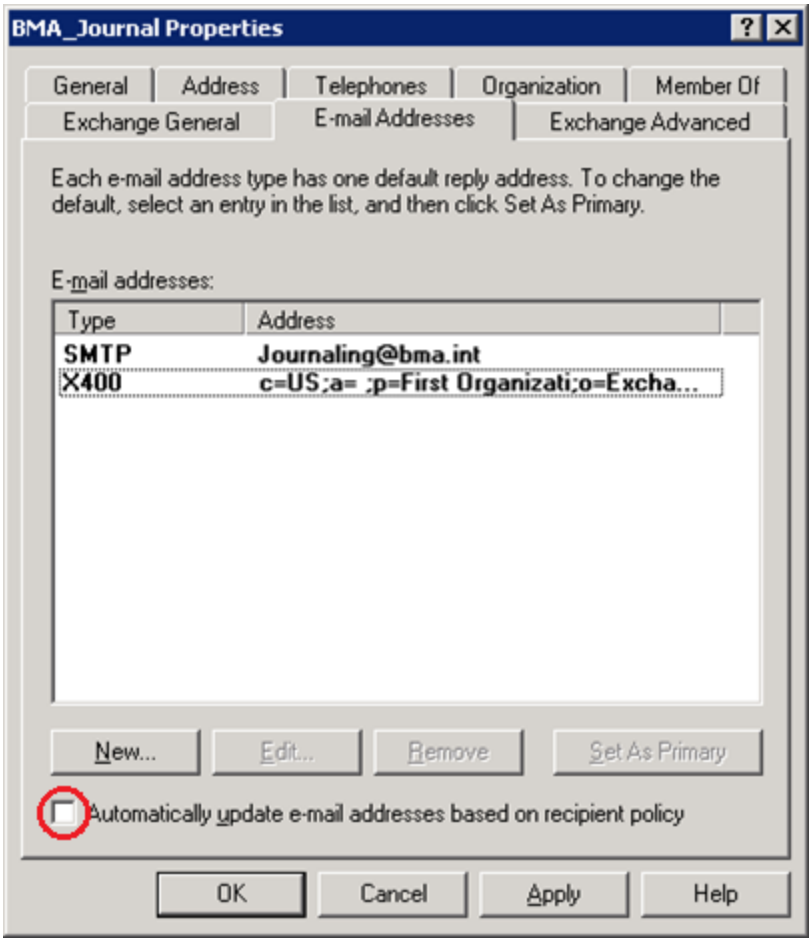


6h. Click **OK**. Click **Apply** in the **Properties** dialog box, and then click **OK** to close the dialog.

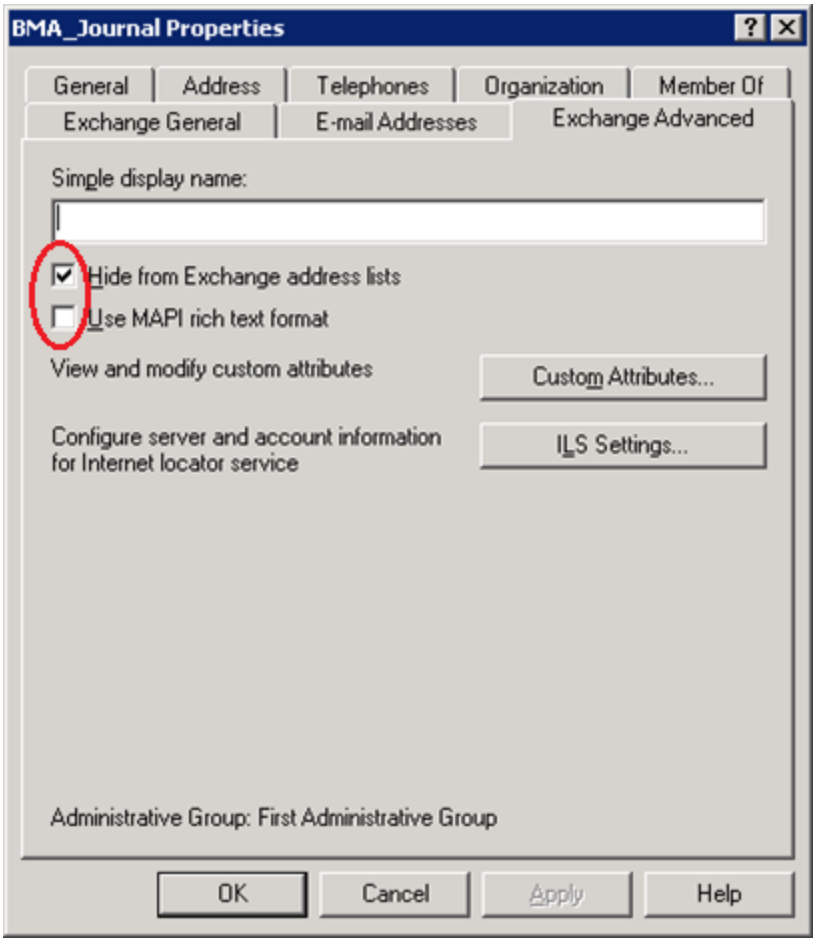
Step 7. Modify Journal Mail Contact

7a. In the **Active Directory Users and Computers** console, right-click on the contact you created in **Step 5**, and click **Properties**.

7b. Click the **E-mail Addresses** tab, and remove all addresses except **journaling@bma.int** and the **X400** address. Clear **Automatically update e-mail addresses based on recipient policy**:



7c. Click **Apply**. Click the **Exchange Advanced** tab, select **Hide from Exchange address lists**, and clear **Use MAPI rich text format**:



7d. Click **Apply**, and click **OK** to close the dialog box.

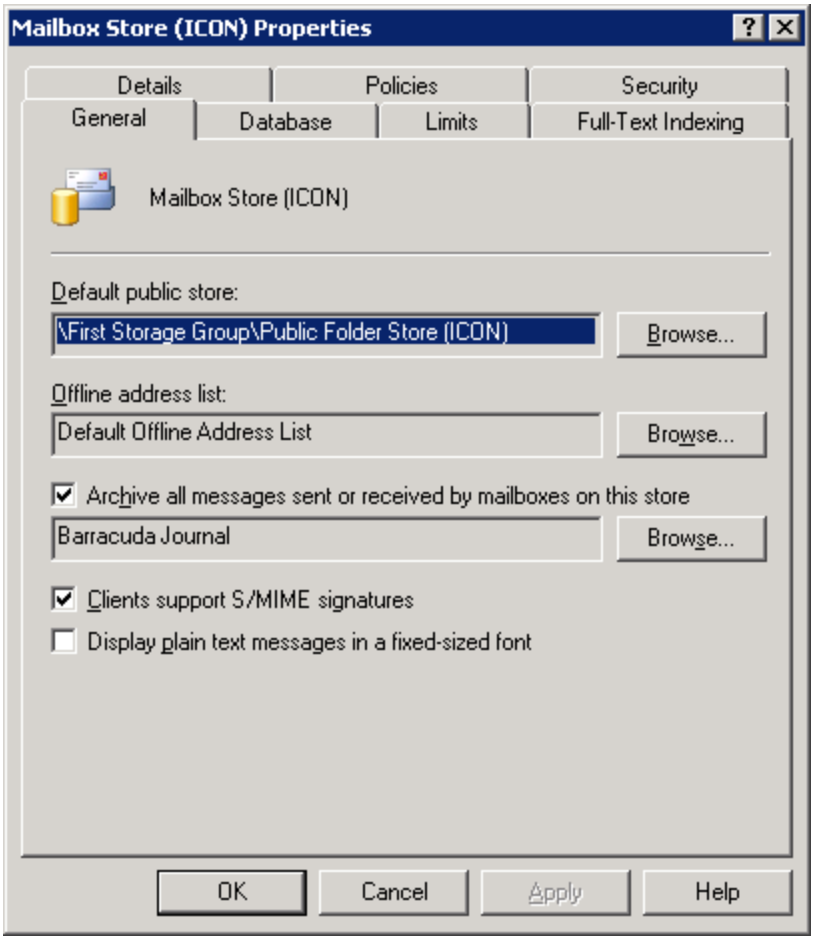
Step 8. Enable Envelope Journaling on Mail Storage

8a. From the Microsoft website, navigate to the **E-Mail Journaling Advanced Configuration tool** ? Unknown Attachment , and complete the following to enable envelope journaling:

- Click **Download**, and save the file **Exejcfg.exe** to a directory on the system, and take one of the following actions to run the executable:
  - Click **Open** *or*
  - Click **Run this program from its current location** *or*
  - At a command prompt, navigate to the file directory, and run the following command: `Exejcfg.exe -e`

8b. Once Envelope Journaling is enabled, in the **ESM**, locate the **Mailbox Store** for your domain, right-click **Mailbox Store**, and click **Properties**.

8c. On the **General** tab, select **Archive all messages sent or received by mailboxes on this store**, and click **Browse** following the **Barracuda Journal** field to locate and select the Journaling Account Mailbox User you created in **Step 4**:



8d. In the **Enter the object name to select field**, enter the User name, and click **Check Names**. Click **OK**.

8e. Click **Apply**, and click **OK** to close the dialog and save your changes.

Step 9. Configure Exchange Mailbox Management

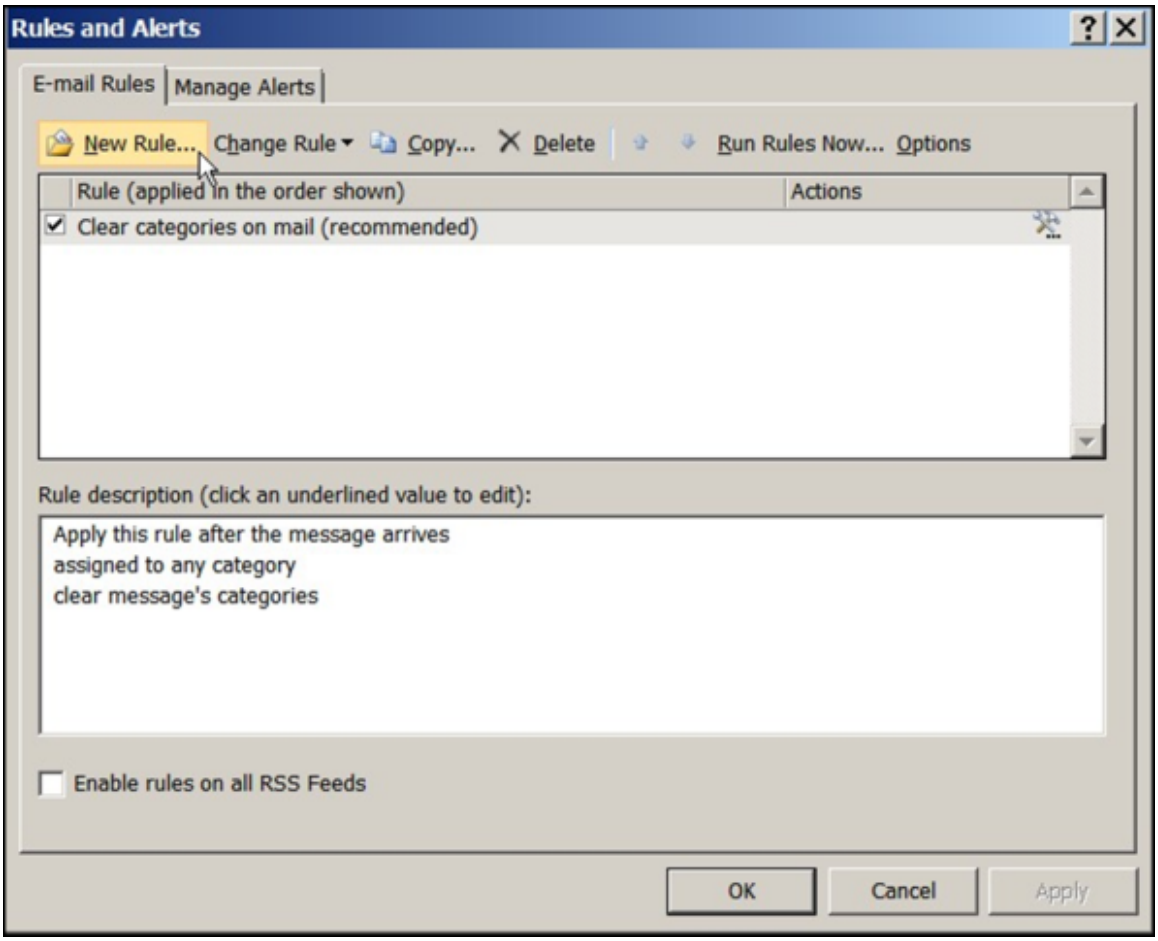
After a message is forwarded to the Barracuda Message Archiver, define an Outlook rule to automatically delete the archived message from the local mailbox store to reduce storage “bloat”.

- Step 9a. Create a Journal Account Mailbox Outlook Rule
- Step 9b. Create Recipient Policy to Delete Messages
- Step 9c. Schedule mailbox Manager to Run Recipient Policy

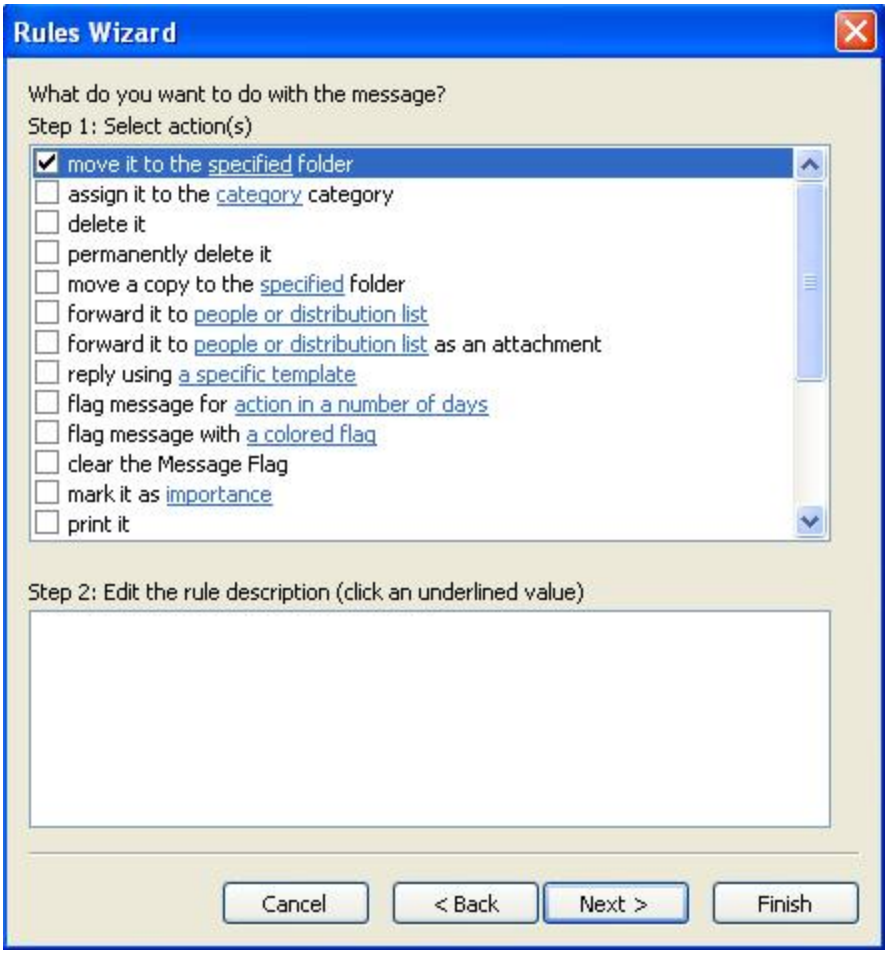
Step 9a. Create a Journal Account Mailbox Outlook Rule

Use the following steps to create an Outlook rule for the Journal Account Mailbox.

1. In Outlook 2003, on the **Tools** menu, click **Rules and Alerts**, click the **E-mail Rules** tab, and click **New Rule**:



2. On the first page of the **Rules Wizard**, click **Start from a blank rule**, and click **Next**.
3. Under **Select when messages should be checked**, select **Check messages when they arrive**, and click **Next**.
4. In the **Select condition(s)** section, verify all conditions are deselected, and click **Next**. Click **Yes** to verify you want to create the rule for all messages that are received in this mailbox.
5. On the next page in the **Select action(s)** section, select **move it to the specified folder**:

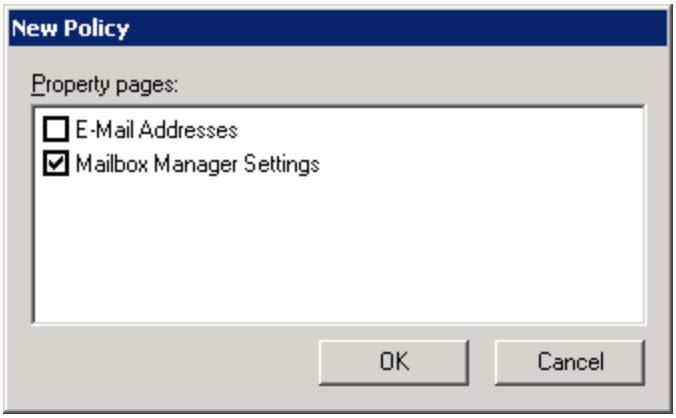

Rules Wizard
What do you want to do with the message?
Step 1: Select action(s)
move it to the specified folder
assign it to the category category
delete it
permanently delete it
move a copy to the specified folder
forward it to people or distribution list
forward it to people or distribution list as an attachment
reply using a specific template
flag message for action in a number of days
flag message with a colored flag
clear the Message Flag
mark it as importance
print it
Step 2: Edit the rule description (click an underlined value)
Cancel
< Back
Next >
Finish

6. In the **Edit** section, click **specified**; the **Rules and Alerts** window displays. Navigate to and select the **Deleted Items** folder, and click **OK** to return to the Rules Wizard. The underlined phrase displays as **Deleted Items**.
7. Click **Finish** to create and activate the Rule.

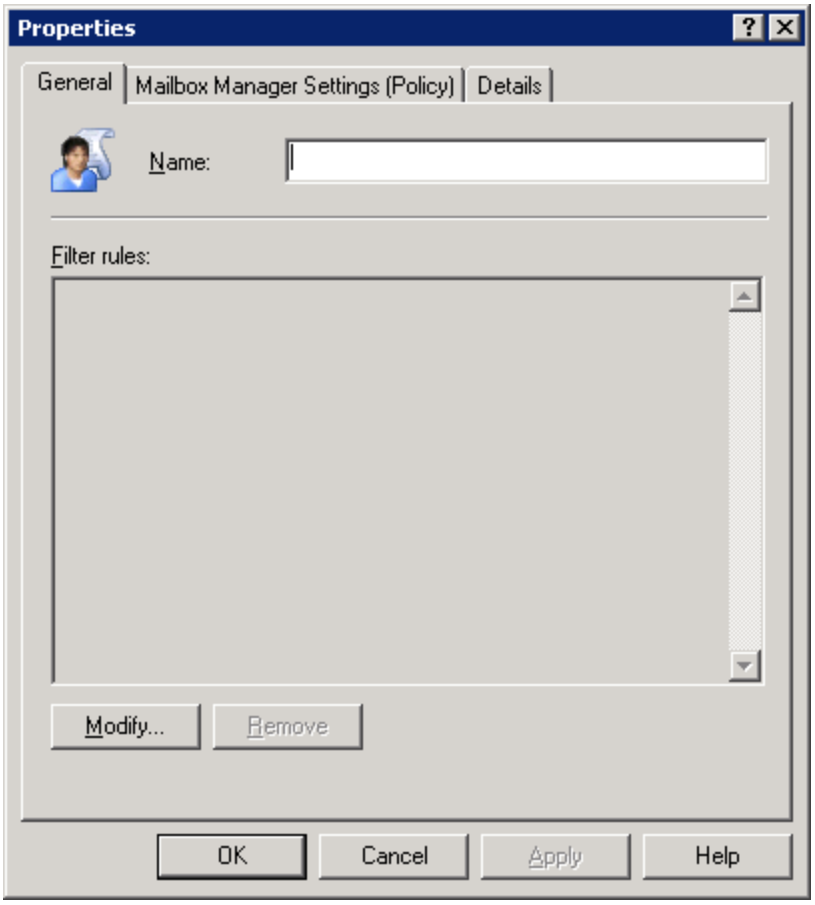
Step 9b. Create Recipient Policy to Delete Messages

Use the following steps to create a recipient policy to delete messages.

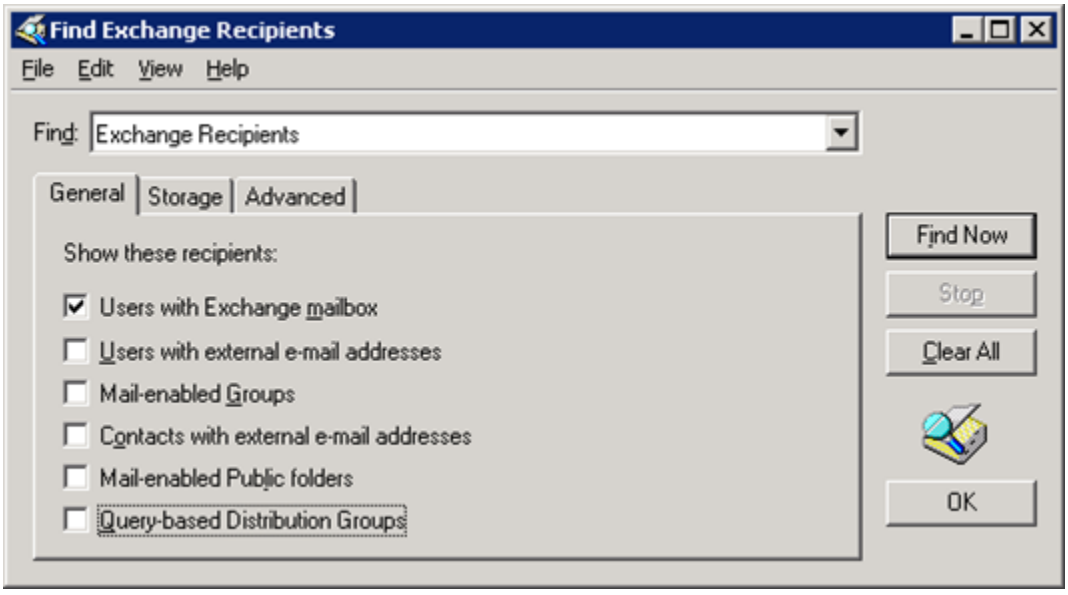
1. In the **ESM** console, expand the **Recipients** folder, right-click on the **Recipient Policies** folder, and click **New > Recipient Policy**.
2. In the **New Policy** dialog box, select **Mailbox Manager Settings**:



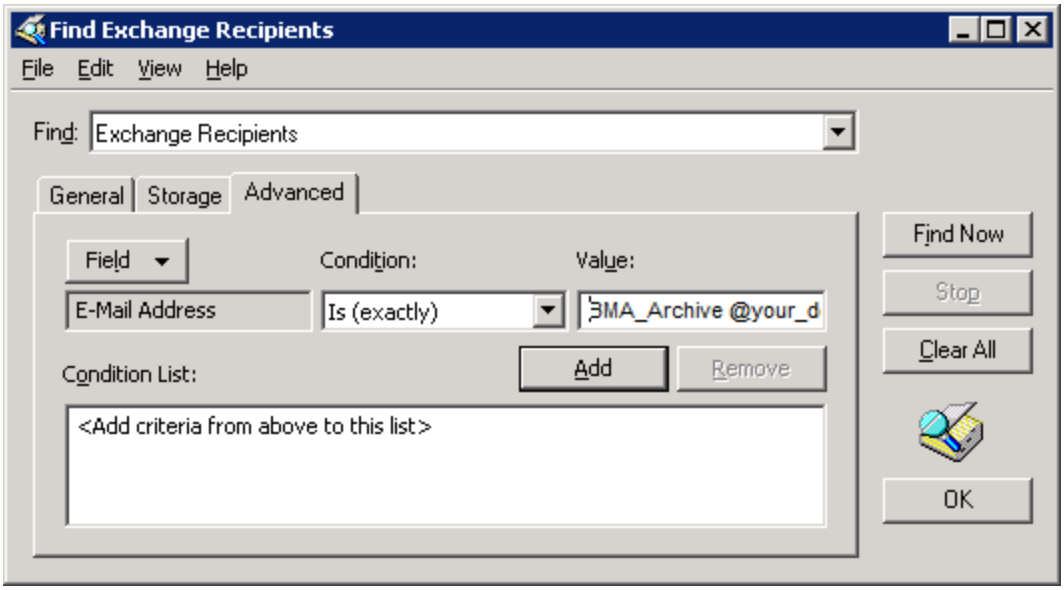
3. Click **OK**; the **Properties** dialog box displays:



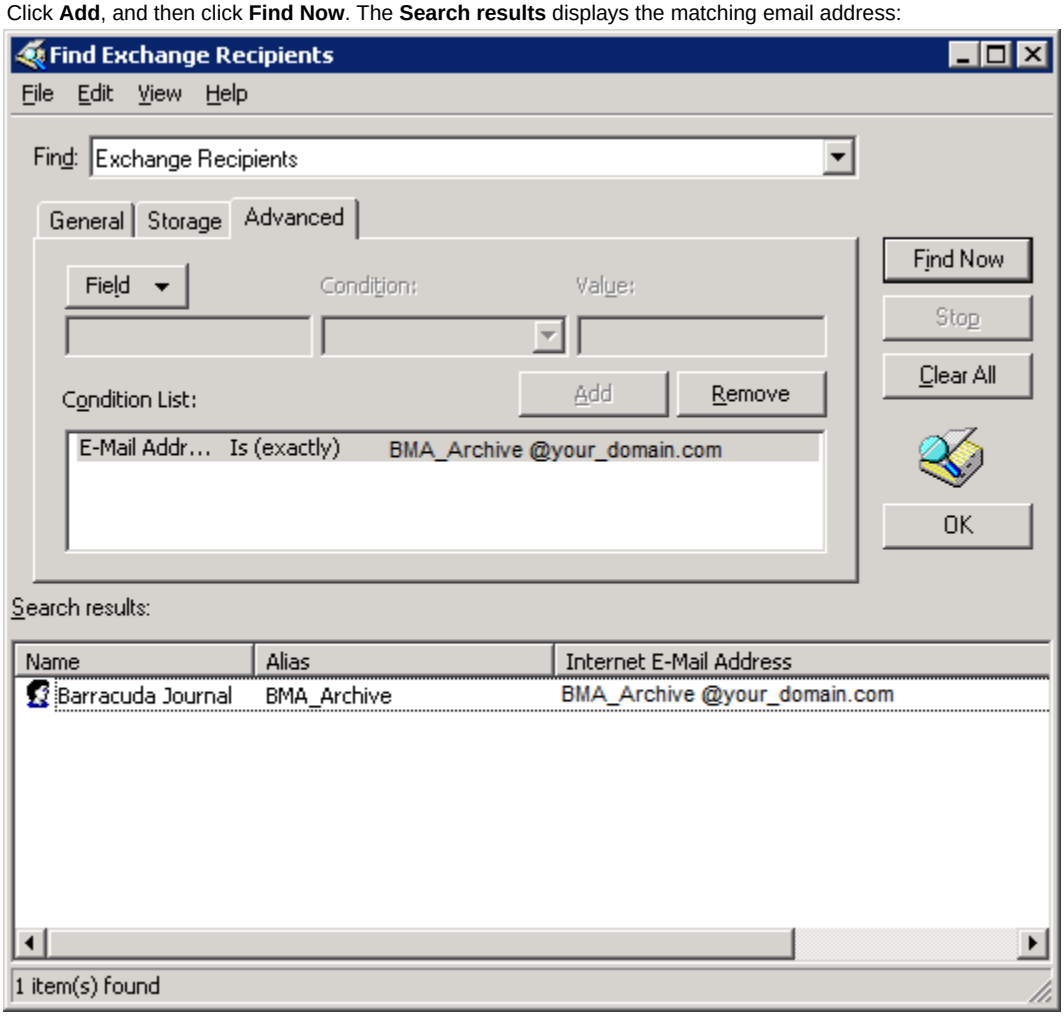
4. On the **General** tab, enter a name for the policy, and click **Modify**; the **Find Exchange Recipients** dialog box displays. Select **Users with Exchange mailbox**, and clear the remaining options:



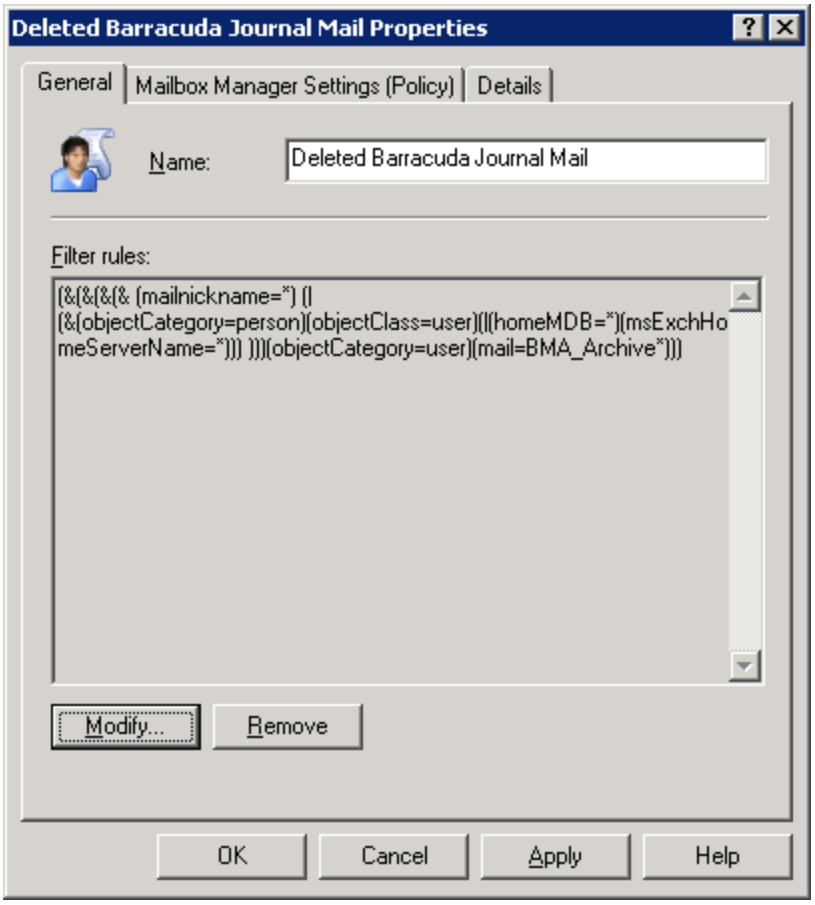
5. Click the **Advanced** tab, and set the following conditions:
   - **Field** = **E-Mail Address**
   - **Condition** = **Is (exactly)**
   - **Value** = `BMA_Archive@your_domain.com`



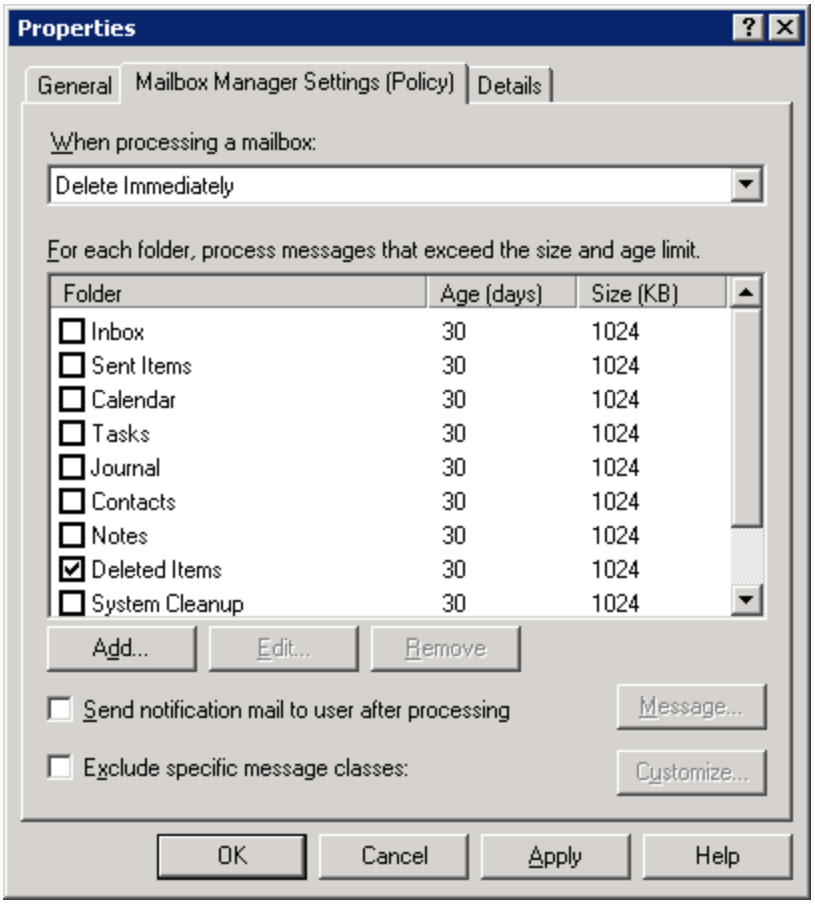
6. Click **Add**, and then click **Find Now**. The **Search results** displays the matching email address:



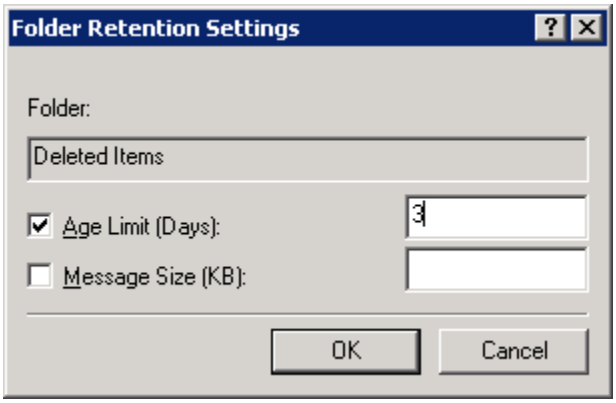
7. Click **OK**. The filter rules display in the **General** tab in the **Properties** dialog box:



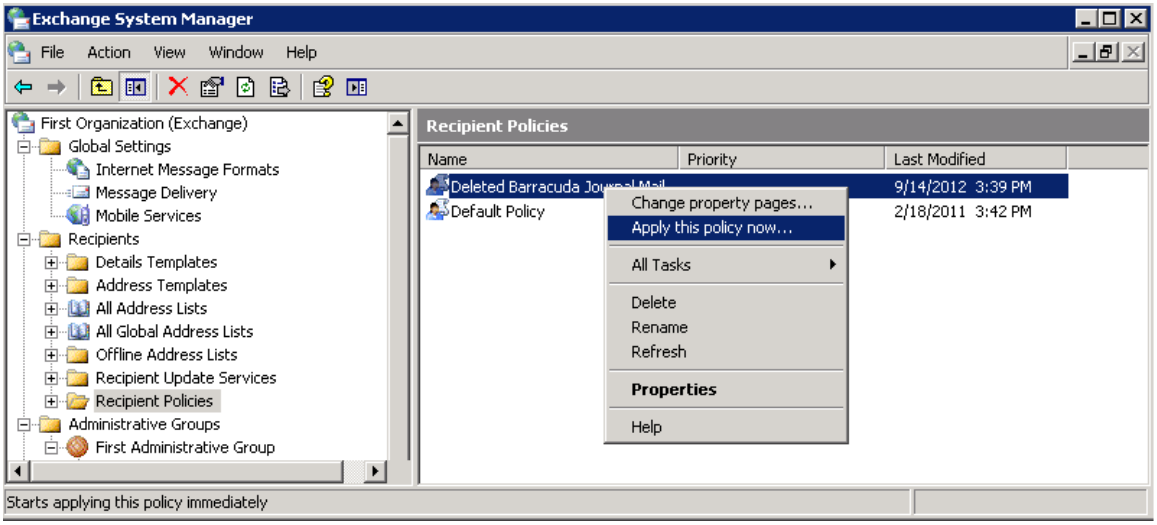
8. Click the **Mailbox Manager Settings (Policy)** tab, and set the following options:
    - From the **When processing a mailbox drop-down**, select **Delete Immediately**.
    - In the **Folder** list, select **Deleted Items**, and deselect the remaining folders:



- Click the **Deleted Items** entry, and click **Edit**; the **Folder Retention Settings** dialog box displays.
- Select **Age Limit (Days)**, and enter an appropriate age limit in the associated field. The specified age refers to the length of time a message remains in the **Deleted Items** folder not when the message was received into Exchange.
- Clear **Message Size (KB)**:



9. Click **OK** to return to the **Properties** dialog box, and then click **OK** to close the dialog.
10. In the **ESM** console, in the **Recipient Policies** details pane, right-click on the newly created policy, and select **Apply this policy now**:

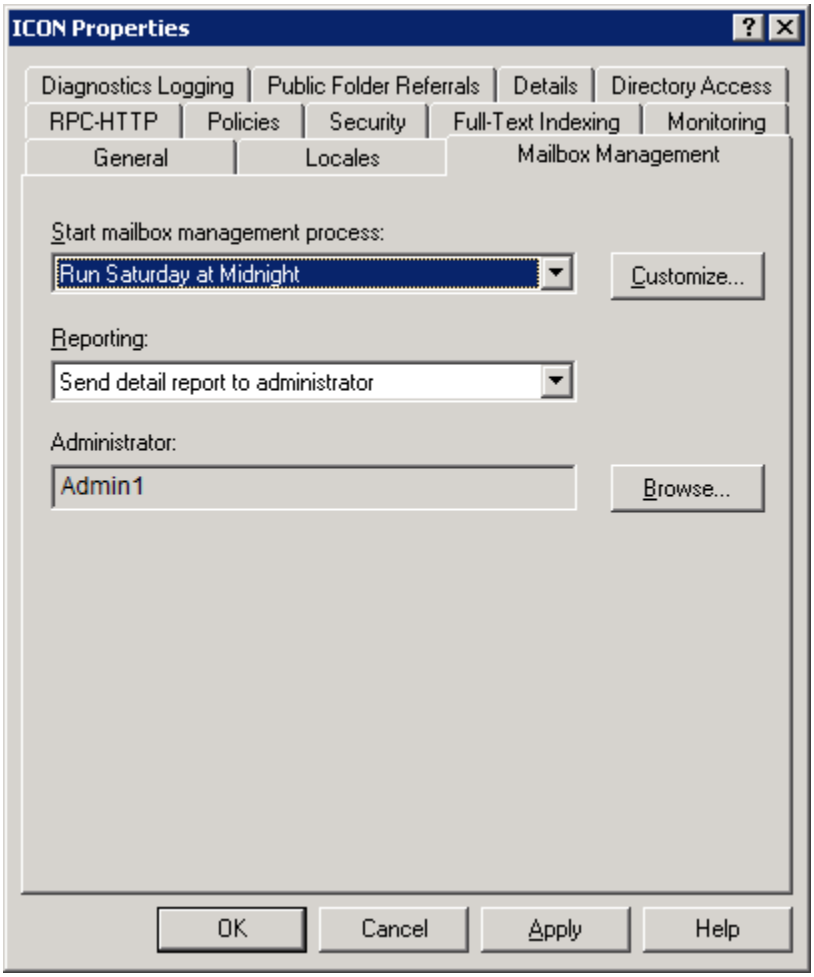


11. Click **Yes** to confirm you want to apply the policy immediately. Once the policy is created, you must schedule the policy to run on each journaling mailbox server that hosts a Journal Account Mailbox as described in **Step 9c**.

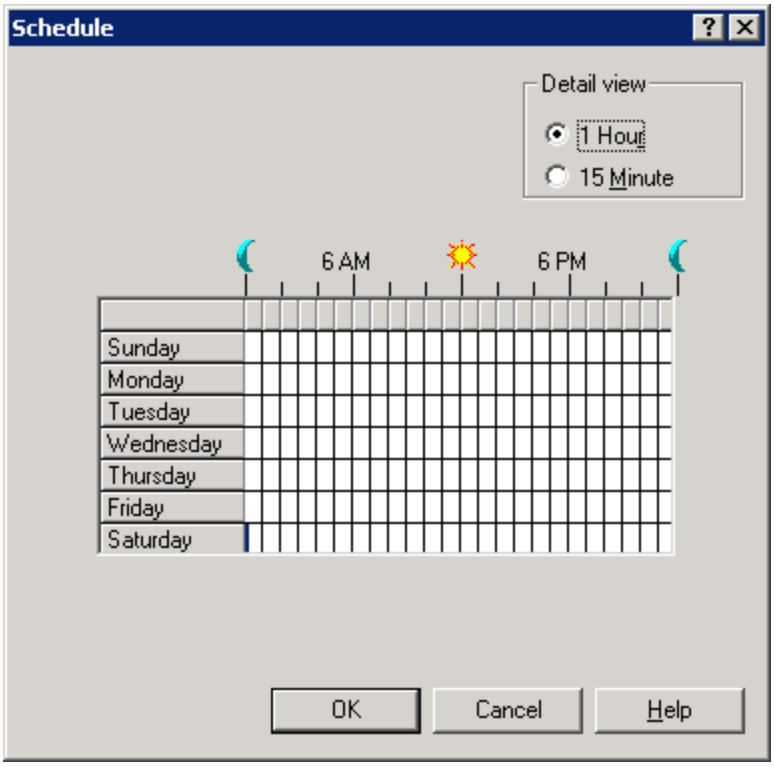
Step 9c. Schedule Mailbox Manager to Run Recipient Policy

Use the following steps to schedule the policy to run on each journaling mailbox server that hosts a Journal Account Mailbox.

1. In the **ESM** console, locate and right-click the name of the server hosting the mailbox on which to run recipient policies, and click **Properties**.
2. Click the **Mailbox Management** tab, and from the **Start mailbox management process** drop-down menu, select the frequency for running the mailbox recipient policies on the server:



3. To customize the frequency of the policy, click **Customize**:



4. Click in the schedule to specify day(s) and time(s), and click **OK** to save your settings.
5. Click **Apply**, and click **OK** to close the **Properties** dialog box.

Step 10. Verify Journaling is Functioning as Expected

Use the following steps to verify journaling is set up and functioning as expected.

10a. Log in to the Barracuda Message Archiver as the administrator.

10b. View the **BASIC > Status** page and verify messages are being processed in the **Message Statistics** table.

- Log in to your email system and send a test email to yourself.
- Go to the Barracuda Message Archiver web interface.
- On the **BASIC > Status** page, in the **Message Statistics** table, recheck the status count; the **Total Messages** count should reflect your test message.
- If the message count does not indicate journaling is operating, verify your administrative settings are properly configured.

10c. On the **ADVANCED > Syslog** page, below the **Mail Syslog** table, click **Monitor syslog** to view mailrelated system log output in a new window.

10d. Verify your test message is journaled in the syslog view.

Proceed to How to Set Up Email Journaling to configure your Barracuda Message Archiver.

Creating an Email Service Account for Microsoft Exchange Server 2003

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher, and a Microsoft® Exchange Server 2003.

You can create an email service account for Exchange import integration and message attachment stubbing.

Related Articles
• How to Enable RPC over HTTP Connectivity

Important – Read First
To create an email service account, you will need to:

- Verify the service account has a mailbox, and *is not* hidden in the **Global Address** list.
- (Optional but highly recommended) Establish a user account through OWA or other source before setting up the email service account.
- Verify public folder database exists on the Exchange Server.

Microsoft Exchange 2003

1. Log onto the Exchange Server as the administrator.
2. From the **Start** menu, go to **Start > Programs > Microsoft Exchange > System Manager**.
3. Expand **Administrative Groups > First Administrative Group > Servers**.
4. Right-click the Microsoft Exchange Server name, and then click **Properties**.
5. On the **Security** tab, select the Barracuda service account, and in the **Permissions list**, set the following permissions:
   - **Administer Information Store**
   - **Send As**
   - **Receive As**
6. Click **Advanced** and verify that the option **Allow inheritable permissions from parent to propagate to this object and all child objects** is selected.
7. Click **OK**.
8. Repeat steps 1 through 7 for each Microsoft Exchange Server that is to host mailboxes within the routing group.

Configuring an IMAP4 or POP3 Journal Account for Microsoft Exchange Server 2003

This article refers to the Barracuda Message Archiver firmware version 3.1 or later and Microsoft® Exchange Server 2003.

- If you are using Microsoft Exchange Server 2003 Enterprise Edition, Barracuda Networks recommends deploying your Barracuda Message Archiver using the push method .
- If you are using Microsoft Exchange Server 2003 Standard Edition and licensing restrictions prevent you from setting up the requisite additional mail store, you can set up IMAP or POP3 journal accounts as described in this article.

You can configure the Barracuda Message Archiver to automatically retrieve messages directly from your mail server using the IMAP or POP3 protocol.

In this article:

- Enable IMAP4 or POP3
- Configure Account
- Enable Envelope Journaling on Mail Storage
- Verify the Service is Started
- Configure a Barracuda Message Archiver Journal Account

Related Articles

- Exchange 2003 SMTP Journal Account

Important Notes
If you are migrating to a newer version of Exchange Server, refer to the Barracuda Message Archiver and Microsoft Exchange Server Migration overview for more information.

Important – Ports
Be sure to open the associated port to allow the Barracuda Message Archiver to communicate freely with the Exchange Server:

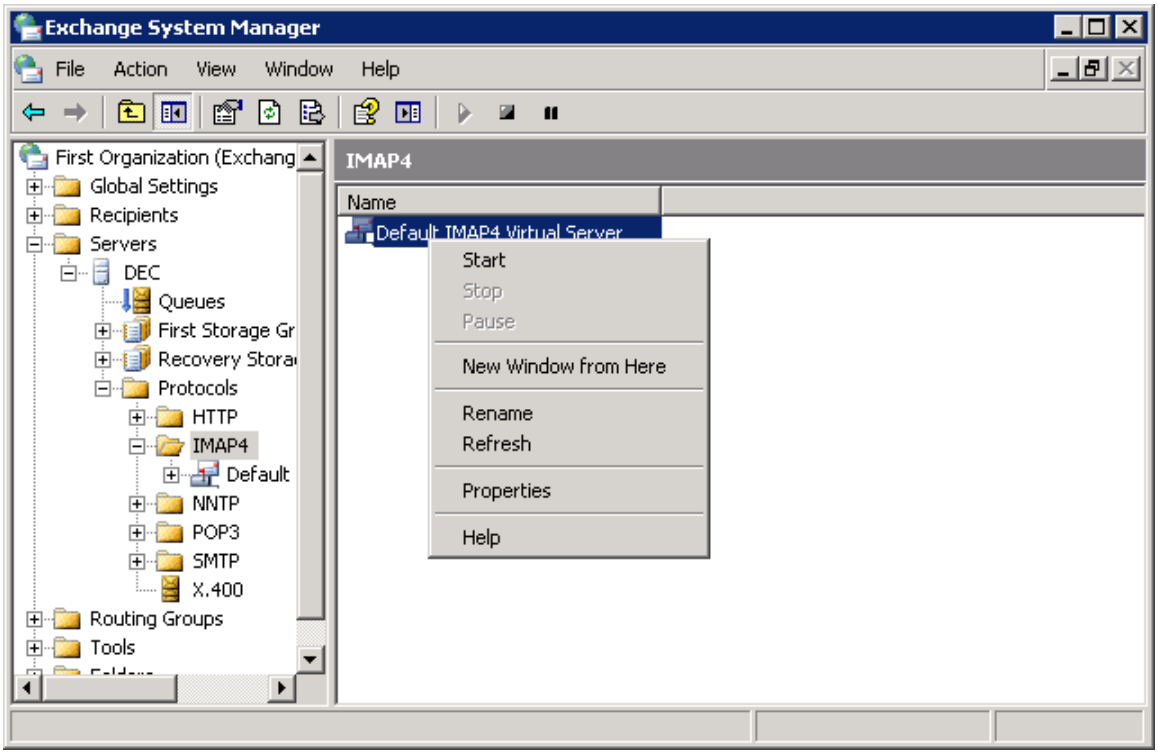
- IMAP4 – Open port 143
- POP3 – Open port 110

Enable IMAP4 or POP3

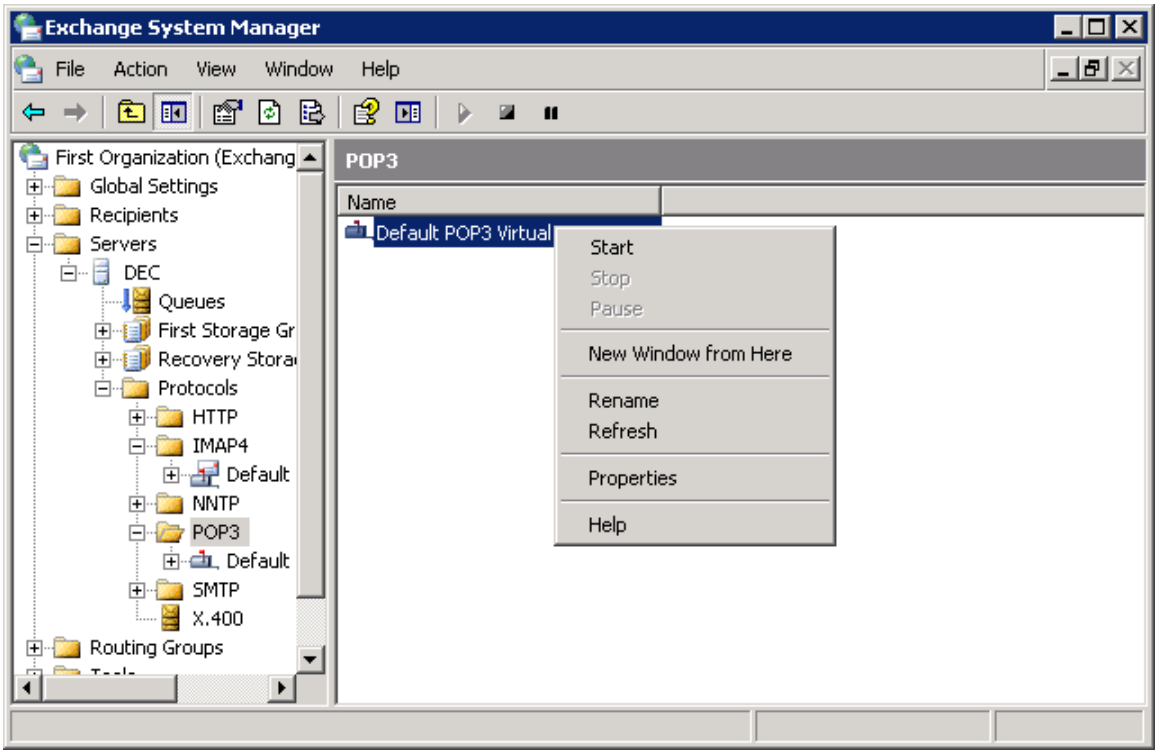
Use the following steps to enable either IMAP or POP3 or your Exchange 2003 Server.

1. Log in to the Exchange Server as the Exchange Server administrator.

2. Launch **Exchange System Manager**, and navigate to **Servers > Protocols > IMAP4**.
3. In the center pane, right-click **Default IMAP4 Virtual Server**, and click **Start**:



4. To enable POP3, navigate to **Servers > Protocols > IMAP4**, and in the center pane, right-click **Default POP3 Virtual Server**, and click **Start**:

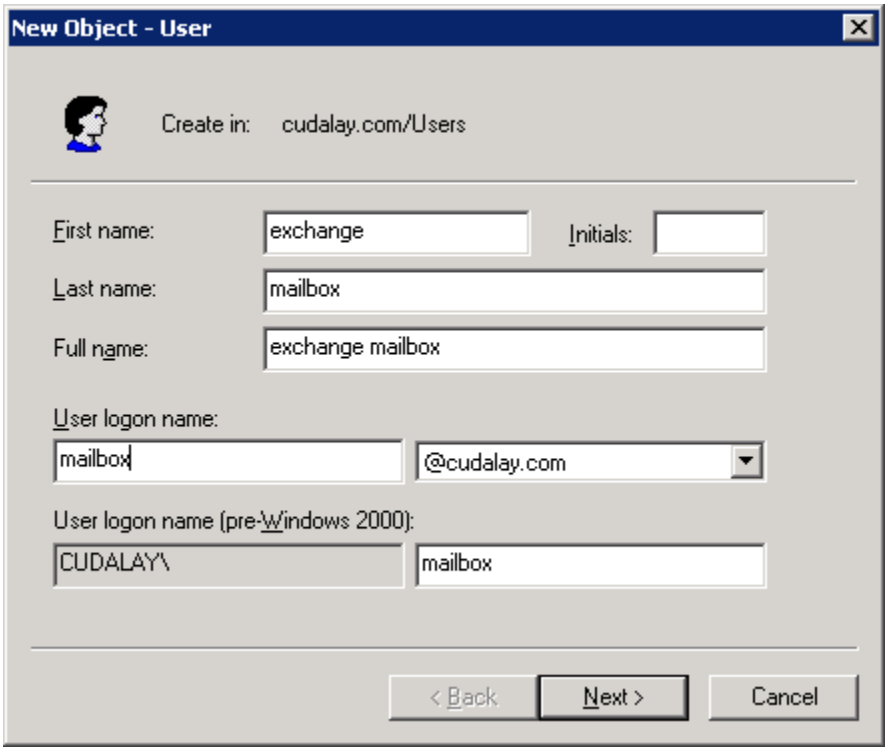


Configure Account

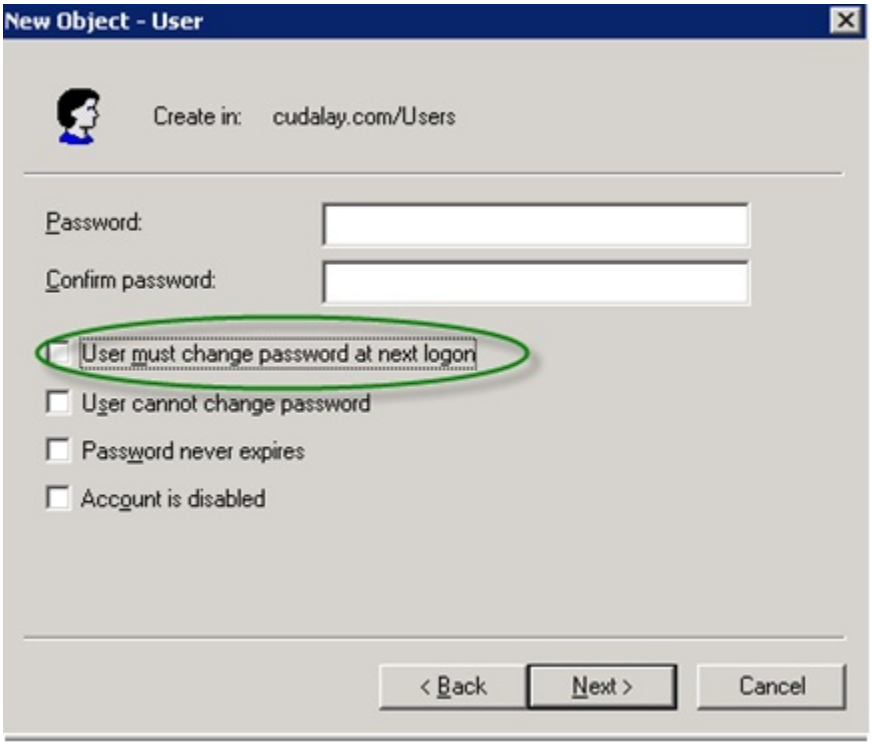
Use the following steps to create an Active Directory (AD) user.

> This account must reside on your organization's domain, not a local machine account.

1. Log in to the Exchange Server as the Exchange Server Administrator.
2. Launch **Active Directory Users and Computers**.
3. Navigate to and right-click **Users**, and click **New > User**; the **New User** dialog box displays.
4. Enter the relevant information to identify the exchange mailbox, and click **Next**:



5. Leave the **Password** field blank, and deselect **User must change password at next logon**:

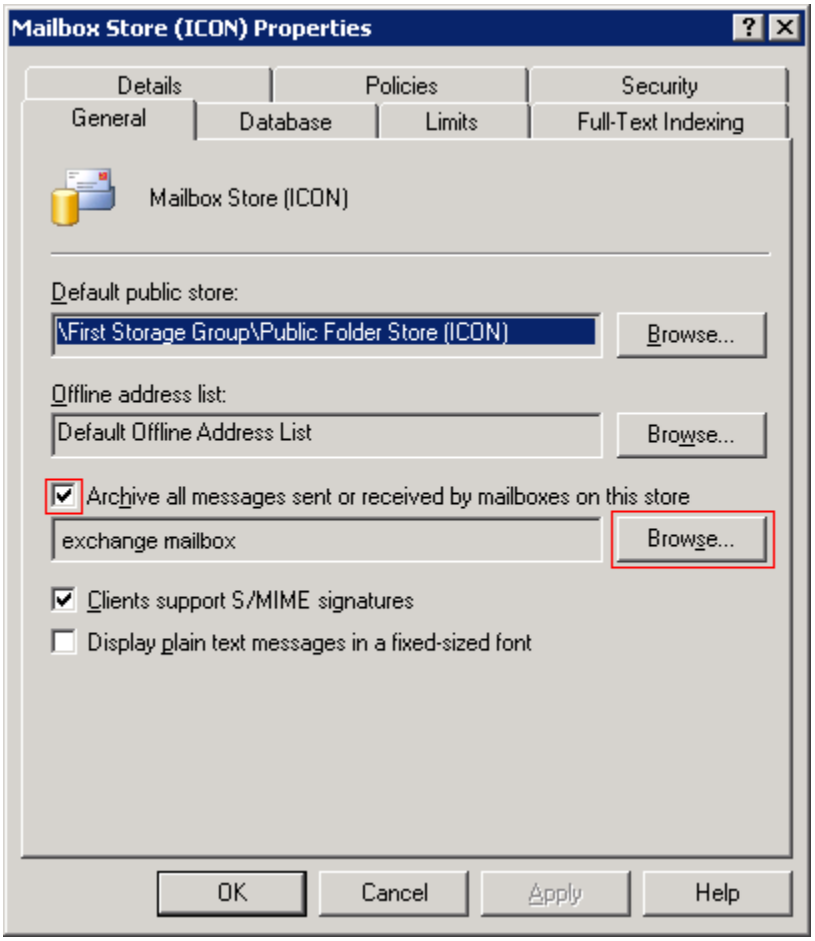


6. Click **Next**. Turn on **Create an Exchange mailbox,** and click **Next**.
7. Verify the user details, and click **Next**, and then click **Finish**.
8. In **Active Directory Users and Computers**, right-click on the newly created Exchange mailbox user, click **Properties**, and click the **E-mail Addresses** tab.
9. Click on the Exchange mailbox name, and click **Set As Primary**.
10. Click **OK** to close the **Properties** dialog box, and save your settings.

Enable Envelope Journaling on Mail Storage

From the Microsoft website, navigate to the E-Mail Journaling Advanced Configuration tool, and complete the following to enable envelope journaling:

1. Click **Download**, save the file **Exejcfg.exe** to a directory on the system, and take one of the following actions to run the executable:
   - Click **Open**; *or*
   - Click **Run this program from its current location**; *or*
   - At a command prompt, navigate to the file directory, and run the following command: `Exejcfg.exe -e`
2. Once Envelope Journaling is enabled, in the **Exchange System Manager** console, locate the **Mailbox Store** for your domain, right-click **Mailbox Store**, and click **Properties**.
3. On the **General** tab, select **Archive all messages sent or received by mailboxes on this store**, and click **Browse** following the Barracuda Journal field to locate and select the Journaling Account Mailbox User created in the previous step:



4. In the **Enter the object name to select** field, enter the **User name**, and click **Check Names**. Click **OK**.
5. Click **Apply**, and click **OK** to close the dialog and save your changes.

Verify the Service is Started

Use the following steps to configure IMAP to accept plain text authentication.

1. Log in to the Exchange Server as the Exchange Server Administrator.
2. Go to **Programs > Administrative Tools > Services**.
3. Verify the selected service status is set to **Started**:
   - **Microsoft Exchange IMAP**
   - **Microsoft Exchange POP3**
4. To change the status, right-click on the service, and click **Start**.

Configure a Barracuda Message Archiver Journal Account

Once you configure the Service Exchange Server, and the service is started, you can add the journal account to the Barracuda Message Archiver

to begin retrieving new messages for archiving. Log in to the Barracuda Message Archiver as the administrator, and go to **MAIL SOURCES > Journal Accounts**.

1. In the **Journal Accounts** section, enter the following details:
   - **Enable Journal Accounts** – Select **Yes** to allow the Barracuda Message Archiver to poll the listed accounts for new messages for archiving.
   - **Enable Journal Testing** – When set to ***Yes*** , all listed accounts are tested for connectivity with each page view**.**
   - **Polling Frequency** – Specify how often to poll each journal account for new messages
2. In the **Journal Accounts Configuration** section, specify the following details for each journal account:
   - **Status** – Displays the connection status for each account.
   - **Server** – Enter the hostname of the mail server where the account resides.
   - **Protocol** – Select whether the account is POP3 or IMAP; once you select the protocol, the default port number automatically populates the **Port** field.
   - **Username** – Enter the complete journaling email address you defined in the section **Configure Account**.
   - **Password** – The password associated with the username defined in the section **Configure Account**.
   - **Encryption** – Select the type of encryption used to connect to the mail server:
     - **TLS (if available)**
     - **TLS**
     - **SSL**
     - **None**
   - **Port** – Select the associated port based on the selected protocol; the default value is port 143 for **IMAP** , and port 110 for **POP3** .
   - **Keep Items on Server** – Select **Keep Items on Server** to allow the Barracuda Message Archiver to automatically clean up the contents of the journal mailbox after each import. When selected, prevents the Barracuda Message Archiver from removing the journaled messages from the mail server; *only* select this option if the contents of the journal account is required by other applications. In this case, make sure that another method for cleaning up the journal account is enabled on the mail server in order to prevent unlimited growth on the mail server and to stay in compliance with your organization's message retention policies.

     > Barracuda Networks recommends that you deselect **keep Items on Server** to save hard drive space on your mail server.

3. Click **Add** to add the journal account; verify the **Status** field displays green, and then click **Save Changes** .
4. To remove a journal account, click the **Delete** ( ) icon, and confirm you want to remove the account.

Creating an Email Service Account for Microsoft Exchange Server 2007, 2010, and 2013

> This article refers to the Barracuda Message Archiver firmware version 3.1 and higher except where noted, and Microsoft® Exchange Server 2007, 2010, and 2013.

You can create an email service account for Exchange import integration and message attachment stubbing.

In this article:

- Microsoft Exchange 2007
- Microsoft Exchange 2010 and 2013

Related Articles

- How to Enable RPC over HTTP Connectivity
- How to Launch Barracuda Message Archiver from Microsoft OWA

Read First

Firmware versions 3.2 and earlier:

To create an email service account, you will need to:

- Verify the service account has a mailbox, and *is not* hidden in the **Global Address** list.
- (Optional but highly recommended) Establish a user account through OWA or other source before setting up the email service account.
- Verify a public folder database exists on the Exchange Server

Firmware versions 3.5 and higher:

To create an email service account, you will need to:

- Verify the service account has a mailbox, and *is not* hidden in the **Global Address** list.
- (Optional but highly recommended) Establish a user account through OWA or other source before setting up the email service account.

Microsoft Exchange 2007

Use the following steps to set the permissions on Exchange 2007:

1. Log in to the Exchange Server as the administrator.
2. From the **Start** menu, go to **Start > Programs > Microsoft Exchange Server 2007 > Exchange Management Shell**.
3. At the command prompt, enter the following command where *Exchange2007* is the name of the Microsoft Exchange 2007 Server and *CUDASVC* is the name of the Barracuda service account, and then press **Enter**: `get-mailboxserver Exchange2007 | add-adpermission -user CUDASVC -accessrights GenericRead, GenericWrite -extendedrights Send-As, Receive-As, ms-Exch-Store-Admin`
4. In the Exchange Management Shell, enter the following command to add View-Only Administrator permissions, replacing *CUDASVC* with the name of the Barracuda service account: `add-exchangeadministrator CUDASVC -role ViewOnlyAdmin`

Important:

If inheritance to the individual mail stores is not enabled on a custom mailbox database, to set the Send As, Receive As, and Administer Information Store permissions at the store level, you must enter the following command in the Exchange Management Shell:
`Add-ADPermission -identity "custom database name" -user "CUDASVC" -accessrights GenericRead, GenericWrite -extendedrights Send-As, Receive-As, ms-Exch-Store-Admin`
To verify the Send As, Receive As, and Administer Information Store permissions, enter the following command in the Exchange Management Shell, where *Exchange2007* is the name of the Microsoft Exchange 2007 Server, *dbname* is the name of the Exchange mail database, and *CUDASVC* is the name of the Barracuda service account**:**

```
get-mailboxdatabase Exchange2007\dbname | get-ADpermission -user CUDASVC | Format-List
```

Microsoft Exchange 2010 and 2013

Use the following steps to set the permissions on Exchange 2010 or 2013 where *database name* is the name of the Microsoft Exchange Server and *CUDASVC* is the name of the Barracuda service account:

1. Log in to the Exchange Server as the administrator.
2. From the **Start** menu, go to **Start > Programs > Microsoft Exchange Server 2010 > Exchange Management Shell**.
3. At the command prompt, enter the following command, and then press **Enter**:
   `Get-MailboxDatabase | Add-ADPermission -User "CUDASVC" -AccessRights ExtendedRight -ExtendedRights Receive-As, ms-Exch-Store-Admin`
   `Add-RoleGroupMember "Organization Management" -Member "CUDASVC"`

Use the following steps to apply permissions for the service account to a specific MailStore database rather than all databases:

1. Log in to the Exchange Server as the administrator.
2. From the **Start** menu, go to **Start > Programs > Microsoft Exchange Server > Exchange Management Shell**.
3. At the command prompt, enter the following command, and then press **Enter**:

```
Get-MailboxDatabase -Identity database name| Add-ADPermission -User "CUDASVC" -AccessRights
ExtendedRight -ExtendedRights Receive-As, ms-Exch-Store-Admin
```

High Availability Deployment

> **Caution**
> High availability (HA) is an advanced feature and may not be appropriate for all environments; contact Barracuda Networks Technical Support *before enabling this feature*.

In this Section

- Understanding Barracuda Message Archiver High Availability
- How to Prepare Systems for High Availability
- How to Join Systems in a High Availability Configuration
- How to Make Changes to an Existing High Availability Cluster
- How to Update Firmware and Energize Updates
- How to Remove or Replace a System

? Unknown Attachment cluster, clustering

Understanding Barracuda Message Archiver High Availability

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher. The High Availability (HA) environment is available on the Barracuda Message Archiver model 450 and higher.

In this article:

- Barracuda Message Archiver High Availability Overview
- Deployment Modes
- Retention Policies and Litigation Holds
- Message Import, Copy, and Search in a High Availability Configuration
  - Message Import and Copy
  - Message Search
  - Offline System in a High Availability Configuration
- Load Balancing

Related Articles

- Prepare Systems for HA
- Join Systems in a HA Configuration
- Update Firmware and Energize Updates
- How to Make Changes to an Existing HA Configuration
- Remove or Replace a System

Additional Resource

- Barracuda Networks Knowledgebase Solution #00006183

Important
High Availability (HA) is an advanced feature and may not be appropriate for all environments; it is *highly* recommended that you contact Barracuda Networks Technical Support before enabling this feature.

Barracuda Message Archiver High Availability Overview

You can join together two Barracuda Message Archivers for HA in order to maximize uptime, provide data redundancy, and reduce the chances of data loss due to system failure.

Deployment Modes

Your deployment mode is usually dependent on the email server configuration that currently exists at your site as well as the number of domains that are to be archived. Following are the two most typical deployment methods for joining Barracuda Message Archivers in an HA configuration.

- **Journaling Deployment** – Both of your Barracuda Message Archivers you want to join in an HA configuration are configured to use either a remote journal account to pull messages to be archived, or a special designated SMTP recipient to push messages to the Barracuda Message Archivers.
- **SMTP (or SMTP Relay) Deployment** – You have a mail server that is not capable of journaling, and you have a Barracuda Spam Firewall installed.

If your email server *does not* support journaling and you *do not* have a Barracuda Spam Firewall, or if you want to join a Barracuda Message Archiver using a *journaling deployment* with a Barracuda Message Archiver using an *SMTP deployment*, contact Barracuda Networks Technical Support for High Availability configuration options.

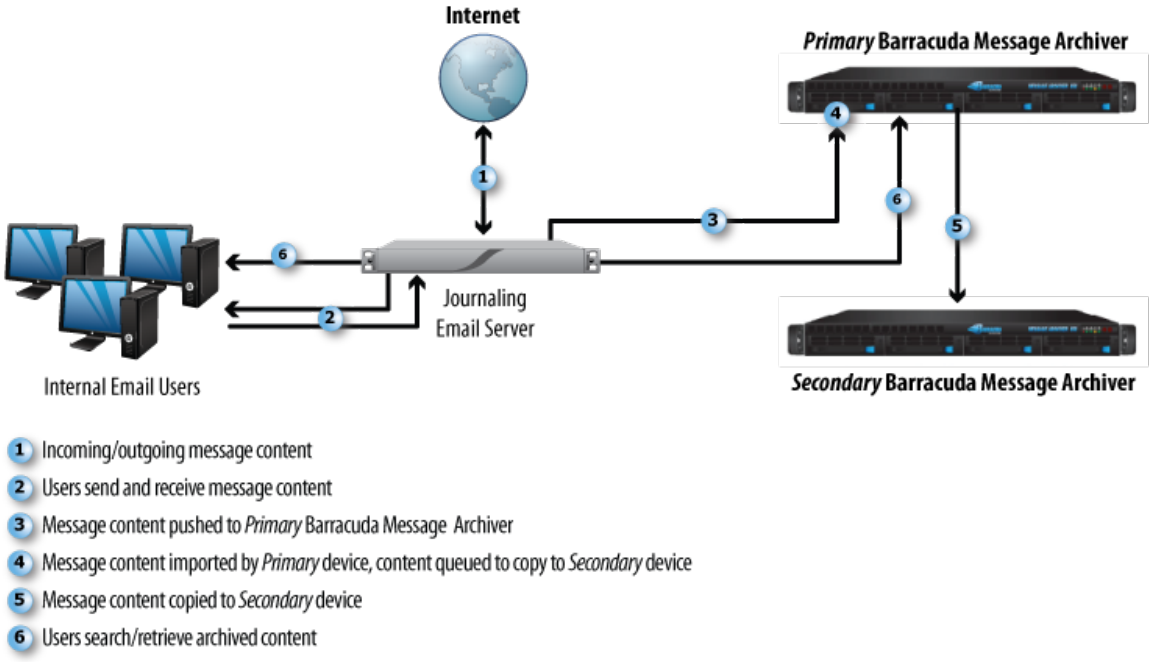
Retention Policies and Litigation Holds

Barracuda Message Archivers joined in an HA configuration act as independent systems with the addition of messages copied from the HA peers. Ensure that retention policies and litigation holds are compatible so as to obtain the same search results on the joined systems.

Message Import, Copy, and Search in a High Availability Configuration

The following figure illustrates message import, copy, and search in an HA configuration.

Figure 1. Message Import, Copy, and Search.


Internet
Primary Barracuda Message Archiver
Journaling
Email Server
Internal Email Users
Secondary Barracuda Message Archiver
1 Incoming/outgoing message content
2 Users send and receive message content
3 Message content pushed to Primary Barracuda Message Archiver
4 Message content imported by Primary device, content queued to copy to Secondary device
5 Message content copied to Secondary device
6 Users search/retrieve archived content

Message Import and Copy

All messages imported into a Barracuda Message Archiver in an HA configuration, regardless of the mail source, are copied to the HA peer. New messages on each system are fully indexed by message content and attachments, and those messages are queued for copy to the other system in the HA configuration. Because message import takes precedence over message copy to an HA peer, queued copy tasks are deferred until there is a *pause* in new mail import tasks. To view the number of messages waiting to be processed, go to the **BASIC > Status** page and view the **Cluster Status**. Note that copy tasks do not display in the **Index Queue Length** metric on the **BASIC > Status** page.

> PST files are *not* transferred between systems, but the messages contained therein are transferred. When a PST file is imported, the Barracuda Message Archiver extracts the messages from the PST file. Those messages are then archived on the primary device and transferred during the archiving process to the secondary device in the HA configuration.

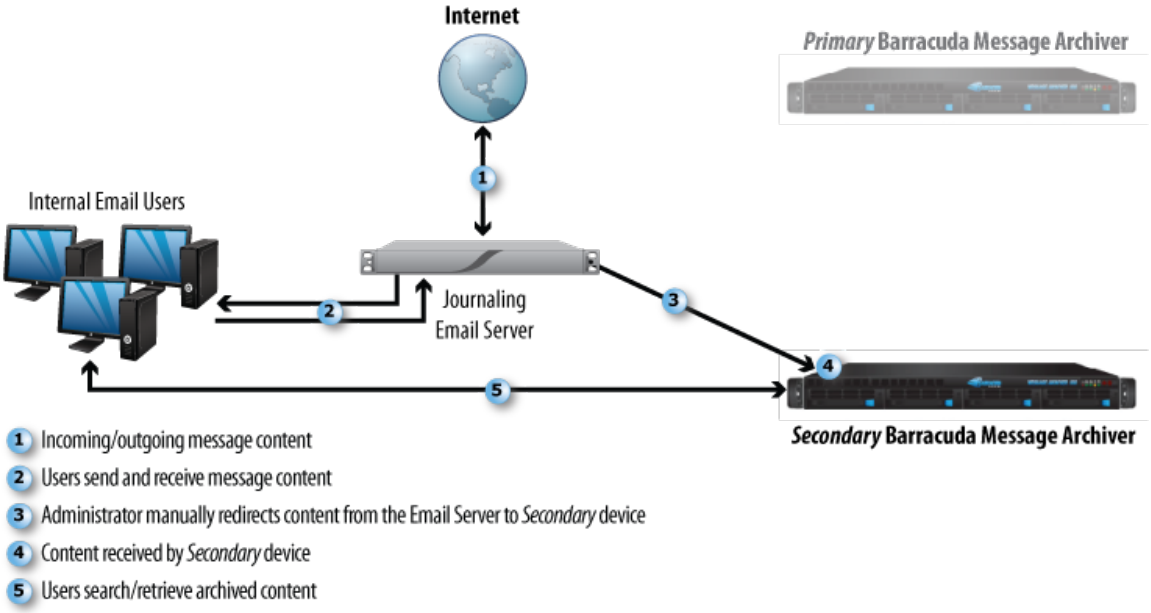
Message Search

Once messages are copied to the HA peer, the messages are available for search on all joined systems. Search results on the HA peer are limited to the items archived on the system, whether imported from a mail source or pushed from one system to an HA peer.

Offline System in a High Availability Configuration

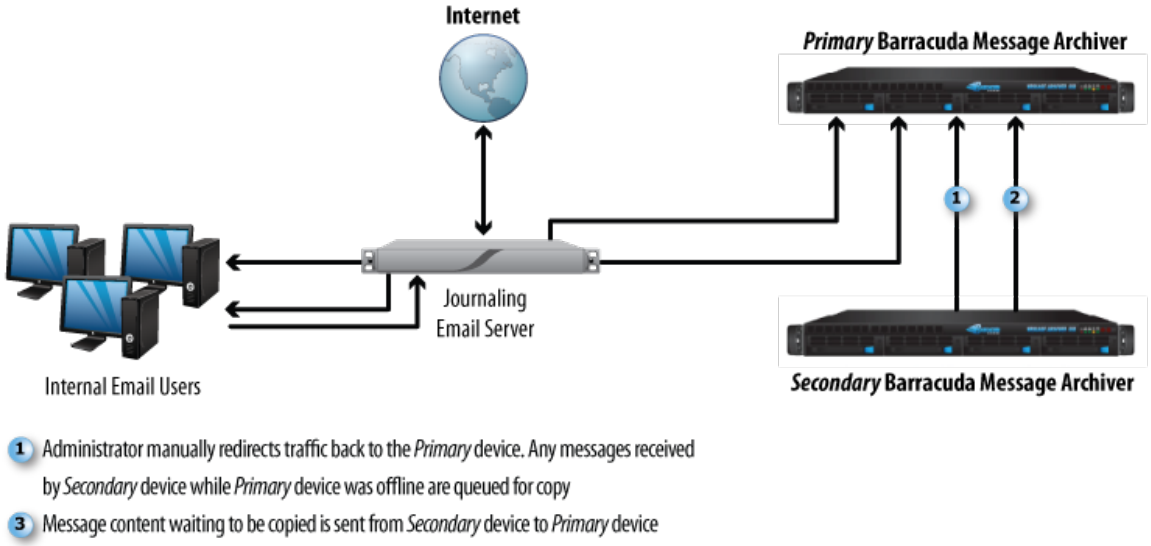
If a system in the HA configuration goes offline, its mail sources are not imported unless you configure another system to import from those same sources. The HA peer continues to archive, and messages waiting to be copied to the offline system are deferred and retried indefinitely until the system is back online.

Figure 2. Primary Barracuda Message Archiver in HA Configuration is Offline.


Internet
Primary Barracuda Message Archiver
Internal Email Users
Journaling Email Server
Secondary Barracuda Message Archiver
1 Incoming/outgoing message content
2 Users send and receive message content
3 Administrator manually redirects content from the Email Server to Secondary device
4 Content received by Secondary device
5 Users search/retrieve archived content

Once the system is back online, it resumes polling its accounts and receiving pushed mail. Any items that were queued to copy to the HA peer resume copying.

Figure 3. Primary Barracuda Message Archiver in HA Configuration is Back Online.


Internet
Primary Barracuda Message Archiver
Journaling Email Server
Internal Email Users
Secondary Barracuda Message Archiver
1 Administrator manually redirects traffic back to the Primary device. Any messages received by Secondary device while Primary device was offline are queued for copy
3 Message content waiting to be copied is sent from Secondary device to Primary device

See View High Availability Status for more information on system status in an HA configuration.

Load Balancing

Barracuda Message Archiver HA does not provide load-balancing functionality; if you have a load balancing device such as the Barracuda Load Balancer, you can configure it to balance the load between the systems in the HA configuration. Use a *Barracuda Load Balancer* to use a single hostname or IP address across the systems in the HA configuration.

How to Prepare Systems for High Availability

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher.

In this article:

- Step 1. Complete the Installation Process
- Step 2. Back Up System Configuration
- Step 3. Verify Firmware Version
- Step 4. Verify Processes are Complete

Related Articles

- Join Systems in HA
- Update Firmware and Energize Updates
- How to Make Changes to an Existing HA Configuration
- Remove or Replace a System

Each Barracuda Message Archiver must function independently before it can be joined to another system for High Availability (HA). Both systems must be able to accept and archive messages, locate each other in the network, and be running the same firmware version.

For the systems you want to include in the HA configuration, perform the steps outlined in this article.

Step 1. Complete the Installation Process

For details on installing the Barracuda Message Archiver, refer to the Barracuda Message Archiver Quick Start Guide**.** Complete the steps in this guide for both Barracuda Message Archiver you intend to include in the HA configuration.

Step 2. Back Up System Configuration

Log into the systems you want to include in the HA configuration and use the **ADVANCED > Backup** page to complete the system configuration backup.

Step 3. Verify Firmware Version

Both Barracuda Message Archivers in the HA configuration must be on the same firmware version. To update the firmware version on joined systems, refer to the article How to Update Firmware and Energize Updates.

Log into each system, and on the **ADVANCED > Firmware Update** page, verify the **Current Installed Version** is the same on both systems. If a system is running an *older* version of firmware, complete the following steps on that system:

1. Log into the system on which to update the firmware, and from the **ADVANCED > Firmware Update** page, download the firmware.
2. Click **Apply Firmware**; once the update is complete, the system reboots.
3. After the system reboots, verify that the firmware has been applied successfully and that the unit is operating as expected.
4. Repeat steps 1 through 3 for each system on which the firmware must be updated.

Step 4. Verify Processes are Complete

For both systems you want to include in the HA configuration, log into the web interface, and verify that no processes are running on the **ADVANCED > Task Manager** page.

Your systems are now ready to join in an HA configuration.

How to Join Systems in a High Availability Configuration

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher.

In this article:

- Step 1. Configure Barracuda Message Archivers for High Availability
- Step 2. Verify System Connectivity
- Step 3. Join the Systems
- Step 4. View High Availability Status

Related Articles

- Prepare Systems for HA
- Update Firmware and Energize Updates
- Remove or Replace a System

To join together two Barracuda Message Archivers for High Availability (HA), complete the steps outlined in this article.

Step 1. Configure Barracuda Message Archivers for High Availability

1a. On the first system you want to include in the HA configuration, navigate to the **ADVANCED > High Availability** page, and in the **Cluster Settings** section, enter the following details:

- **Cluster Shared Secret** – Enter an alphanumeric shared secret passcode; you must enter the same code on all Barracuda Message Archivers that you want to include in the HA configuration so that the systems 'trust' one another.

  Important
  The passcode *must match exactly* on all systems.

- **Cluster Hostname** (optional) – Enter a DNS name or hostname by which other systems in the HA configuration can reach this system; leave this field empty to use the system IP address.

1b. Click **Save Changes**.

1c. Repeat steps 1a through 1b, using the *same* shared secret for the HA peer system.

Step 2. Verify System Connectivity

Once the Barracuda Message Archivers are fully configured for HA, make sure that each system can see the other system over the network.

2a. Log into each system, and navigate to the **ADVANCED > Troubleshooting** page. In the **Network Connectivity Tests** section, enter the hostname or IP address of the system you want to test in the **Ping Device** field, and click **Begin Ping**.

Important
The hostname *must match* that which you entered in the **Cluster Hostname** field for the other system, or that system's IP address if the field was left blank.

2b. Verify the other system can be seen over the network. Once you have completed the HA settings and verified system connectivity for both Barracuda Message Archivers, you are ready to join the systems into an HA configuration.

Step 3. Join the Systems

3a. Once you configure the HA settings for both system, navigate to the **ADVANCED > High Availability** page on the first system that is to be included in the HA configuration.

3b. In the **Clustered Systems** section, enter the DNS hostname or IP address of the system to which you want to join, and click **Join Cluster**, and click **Save Changes**.

3c. Once joined, the **Clustered Systems** table displays the system in the HA configuration. New messages received by either of the Barracuda Message Archivers in the HA configuration are now available in the Search results on *both* joined systems.

3d. To use a name that is not resolvable by DNS, enter the provided hostname and corresponding IP address in the **Local Host Map** section. This creates a local Host-to-IP mapping for a system in the HA configuration. Enter the **Host Name** and **IP Address** for the joined Barracuda Message Archiver, and click **Add**.

Important
Any entry added in the **Local Host Map** section *overrides* any matches that may be found from a DNS lookup; the information is not synchronized with other systems in the HA configuration.

Step 4. View High Availability Status

You can view the number of messages that are waiting to be processed on the selected Barracuda Message Archiver in the **BASIC > Status** pag e in the **HA Cluster Status** section.

If a system in the HA configuration goes offline, the status button in the **Clustered Systems** table on the **ADVANCED > High Availability** page displays red. Mouse-over the system to view system status. Archiving behavior continues as expected on the remaining system in the HA configuration.

How to Make Changes to an Existing High Availability Cluster

This article refers to firmware version 3.5 and higher.

Important

Firmware release 3.5 and higher synchronizes commonly used configuration settings between appliances in a High Availability (HA) configuration including saved searches, retention policies, and litigation holds. Before moving to firmware release 3.5, confirm that the saved searches, retention policies, and litigation holds are configured the same on all systems in the HA configuration. Additionally, before upgrading the clustered appliances to firmware version 3.5, it is *imperative* that you verify all systems are running the same firmware release. Upgrade clustered systems in a parallel time frame so that data from the primary system continues to reach the secondary system.

Before you perform maintenance upon, or break an HA pair, *contact Barracuda Networks Technical Support* to determine the proper workflow for your environment.

To change the IP address on either appliance in an HA pair:

1. Pause any new mail flow to both appliances in the HA pair including journaling (SMTP or POP/IMAP) as well as Exchange import, stubbing, and data imports such as FolderSync or PIMSync.
2. Make the necessary IP address changes on the appliances.
3. Resume journaling and any other data flows.

Configuration Variables

In firmware 3.5 and higher, many configuration variables automatically synchronize across the cluster. For example, saved searches, retention policies, litigation holds configured on one appliance are also available on the other appliance in the HA pair.

Cluster Variables

The following list describes the cluster variables that are *not synchronized* across an HA pair:

- GroupWise configuration details
- Any Exchange Integration details (for example, stubbing, folder sync, etc.)
- Serial number (this never changes)
- Administrator password
- Guest password
- Whether the latest release notes have been read
- IP Address, Subnet Mask, and Default Gateway (as configured on the **BASIC > IP Configuration** page)
- Primary DNS Server and Secondary DNS Server (as configured on the **BASIC > IP Configuration** page)
- Host Name (as configured on the **BASIC > IP Configuration** page)
- Time Zone (as configured on the **BASIC > Administration** page)
- Web Interface HTTP Port (as configured on the **BASIC > Administration** page); this must be the same value on *all* systems in the cluster
- Any advanced IP configuration (as configured on the **ADVANCED > ADVANCED Networking** page)
- All customized branding (models 650 and above, as configured on the on the **ADVANCED > Appearance** page)
- Cluster Shared Secret; note that this must be the same on *all* systems for the cluster to work properly (as configured on the **ADVANCED > High Availability** page)
- Cluster Hostname (as configured on the **ADVANCED > High Availability** page)
- Local Host Map (as configured on the **ADVANCED > High Availability** page)
- Web Interface HTTPS/SSL port (as configured on the on the **ADVANCED > Secure Administration** page); must be the same value on *a*

ll systems in the cluster
- Any other secure administration configuration, including saved certificates (as configured on the **ADVANCED > Secure Administration** page)
- All SSL information, including saved certificates (as configured on the on the **ADVANCED > Secure Administration** page)

How to Update Firmware and Energize Updates

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher.

In this article:

- Update Firmware Across a High Availability Configuration
- Update Energize Updates

Related Articles

- Prepare Systems for HA
- Remove or Replace a System

Important
Both Barracuda Message Archivers in a High Availability (HA) configuration *must* be on the same firmware version. If you need to update the firmware version on the systems, plan to update *both* systems at the same time.

Before you update the firmware, create a backup of your configuration data from the **ADVANCED > Backup** page on *both* systems prior to starting the firmware update.

Update Firmware Across a High Availability Configuration

Complete the following steps to update the firmware version on each system in the HA configuration:

1. Log into the first system, and from the **ADVANCED > High Availability** page, verify that the systems in the HA configuration display online (all green indicators) in the **Clustered Systems** table.
2. From the **ADVANCED > Backup** page, create a backup of the system configuration.
3. From the **ADVANCED > Firmware Update**page, download the firmware version onto each system.

   Important
   Do not click **Apply Firmware** until the firmware is downloaded to both systems in the HA configuration.
4. Complete steps 1 through 3 for the other system in the HA configuration.
5. Apply the firmware on the first system. After the update is complete and the system reboots, verify that the firmware has been applied successfully and the unit is operating as expected.
6. Repeat steps 4 and 5 for the remaining system in the HA configuration.

Update Energize Updates

Energize Updates (for both firmware and definitions) do not synchronize across the Barracuda Message Archivers in the HA configuration. You must update both systems in the HA configuration individually from the **ADVANCED > Energize Updates** page.

How to Remove or Replace a System

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher.

Typically, there are only two reasons why you would want to remove a system from an HA configuration:

- when you no longer want to maintain HA, or

- when you are replacing one of the systems in the HA configuration.

Related Articles
• Prepare Systems for HA • Join Systems in HA • Update Firmware and Energize Updates

Warning

If you are replacing a Barracuda Message Archiver, it is *highly* recommended that you contact Barracuda Networks Technical Support prior to removing it from a High Availability (HA) configuration. Because of the large volume of data, you must take great caution during the separation process so as to minimize downtime and potential data loss.

Remove a System

1. Log in to the device in the HA configuration that you are *not* removing from the configuration, and use the **ADVANCED > Backup** page to complete the system configuration backup.
2. Log into the Barracuda Message Archiver you want to *remove* from the HA configuration, navigate to the **ADVANCED > High Availability** page, and in the **Cluster Settings** section, complete the following:
   - Change or clear the **Cluster Shared Secret** field.
   - Click **Save Changes**; the Barracuda Message Archiver is now unable to communicate with the other system in the HA configuration, and any messages arriving on the other system after this time are not duplicated on the system you are *removing*.
   - On the system you are *removing*, delete the Barracuda Message Archiver from the **Clustered Systems** table, and click **Save Changes**.
3. On the Barracuda Message Archiver you are *not* removing, navigate to the **ADVANCED > High Availability** page, and delete the *removed* Barracuda Message Archiver entry from the **Clustered Systems** table.

Replace a System

Remove the old device, and install the new replacement device using the Barracuda Message Archiver Quick Start Guide.

Once the new device is installed, follow the steps in the following sections to complete the system replacement in the HA configuration:

1. How to Prepare Systems for High Availability
2. How to Join Systems in a High Availability Configuration

CommuniGate Pro E-Mail Server Deployment

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher, and the CommuniGate Systems ® CommuniGate Pro™ E-Mail Server.

The following email rule specifies that a mirrored copy of an email is created for any email in the queue that is not already destined for the Barracuda Message Archiver. This rule prevents looping of mirrored messages.

Additional Resources
• Barracuda Networks Knowledgebase Solution #0 0003504

Use the following steps to set up the email rule,

1. Log into CommuniGate Pro as the Administrator, and E-mail Queue Rules section, set the following conditions:
   a. **Any Recipient**
   b. **is not**
   c. Enter *<archiver@IP address of your Barracuda Message Archiver>* , for example, enter `archiver@192.168.200.200`
2. Set the action to take is:

a. **Mirror to**
b. Enter <*archiver@IP address of your Barracuda Message Archiver*> , for example, enter `archiver@192.168.200.200`

The Barracuda Message Archiver automatically accepts and archives emails sent from CommuniGate Pro to the address <*archiver@IP address of your Barracuda Message Archiver*>.

Google Apps Deployment

This article refers to the Barracuda Message Archiver release 3.1 or higher, and Google® Apps Business™ and Google Apps Education™ editions.

In this article:

- Create an Archive/Journal Mailbox
- Add Email Settings
- Enable IMAP/POP in Google Apps
- Enable IMAP/POP in Gmail
- Add the Journal Account to the Barracuda Message Archiver

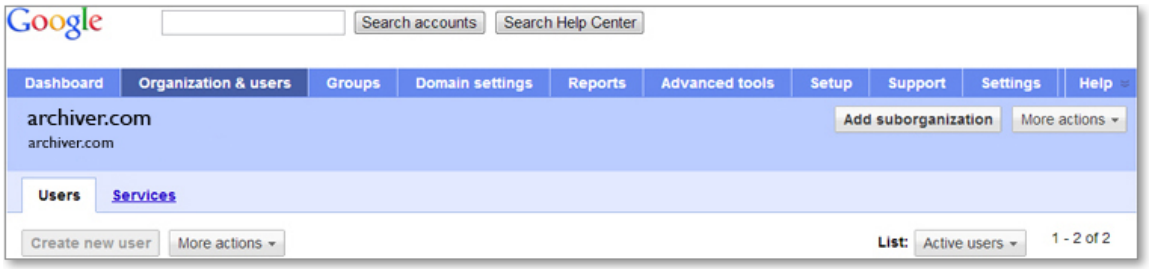
Recommended Deployment

Barracuda Networks recommends deploying your Barracuda Message Archiver with Google Apps using the Barracuda cloud relay service configuration for Google Apps Mail Service, alternately, you can set up IMAP/POP3 journaling as described in this article.

Create an Archive/Journal Mailbox

Use the following steps to create a mailbox to which to archive all email.

1. Log in to the Google Apps administrator control panel as the Administrator.
2. At the top of the page, click **Organization & users**:



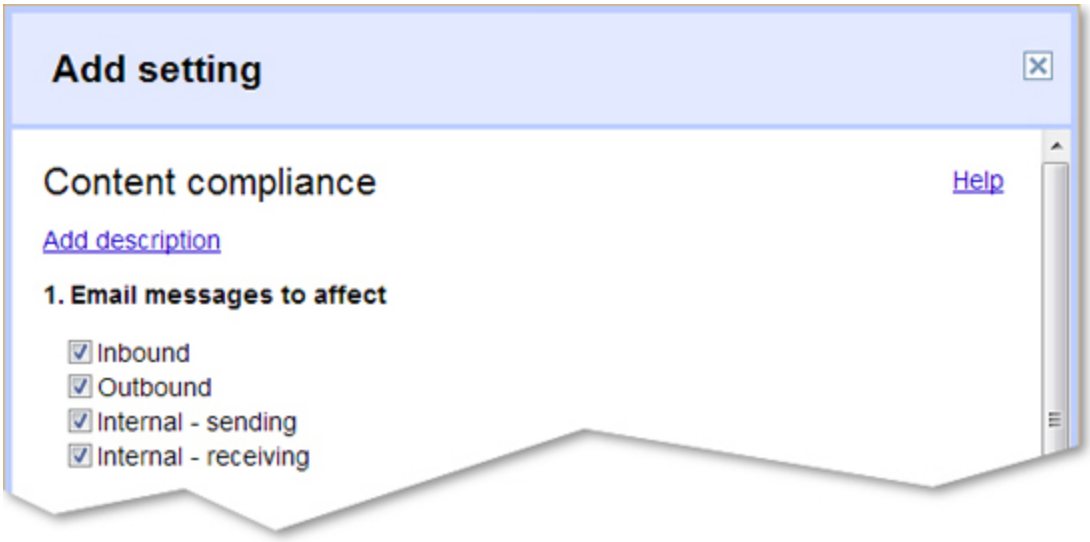
3. Click **Create a new user**. Enter the new user **First Name**, **Last Name**, and **Primary email address** in the appropriate fields.
4. Select the domain you want to journal mail.
5. Click **Set password** to set the initial password; enter the password twice. Note that Google requires the password to be at least eight characters in length.
6. Click **Create new user** to save your settings.

Add Email Settings

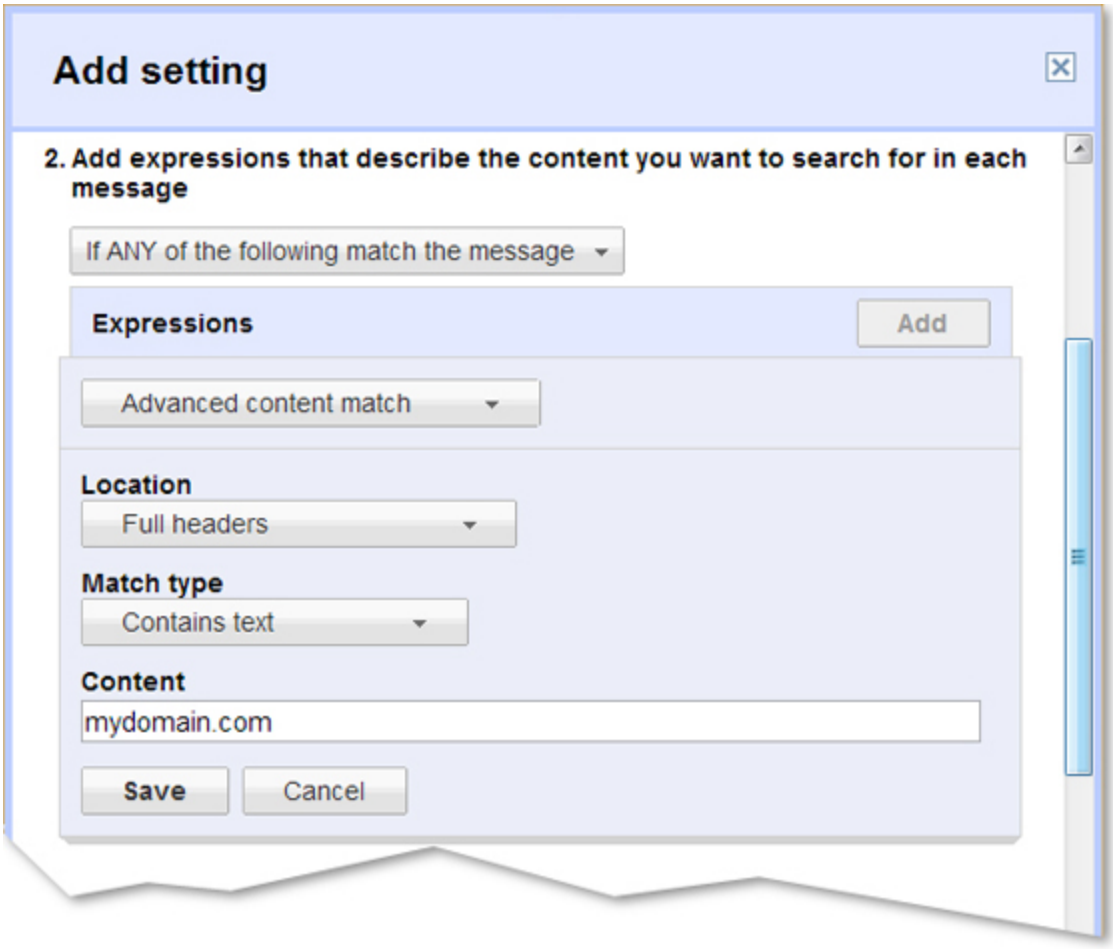
Use the following steps to configure email settings for the Barracuda Message Archiver domain.

1. Sign into the Google Apps control panel as the Administrator.
2. From the menu at the top of the page, select **Settings**.
3. From the left-navigation menu, click **Email**, scroll down to **Content compliance**, and click **Configure**.
4. In the **Add setting** page, select each of the following options to enforce content-based policies for inbound, outbound, and internal emails by matching one or more expressions to different areas of the email, e.g., body, header, and subject:
    - **Inbound**

- **Outbound**
- **Internal – sending**
- **Internal – receiving**



5. **In the Add setting dialog box, in step 2, select If ANY of the following match the message, and under Expressions click Add.**
6. From the drop-down menu, select **Advanced content match**; the Advanced content options display. Select the following options:
    - From **Location** select **Full Headers**.
    - From **Match type** select **Contains text**.
    - In the **Content** field, enter all domain names for which you want to archive mail:



7. Click **Save**.
8. In the **Add setting** dialog box, in step 3, enter the following information:
    - Select **Modify message**.
    - Under **Also deliver to** turn on **Add more recipients**. Click **Add** and enter the email address of the Archive/Journal mailbox created in the section **Create an Archive/Journal Mailbox** including the domain.
    - Select the appropriate domain; select the primary journal mailbox unless you want to set up a mailbox and rule for each domain.
9. Click **Save**.
10. Step 4 (Optional). To bypass the settings in this dialog for messages received from specific addresses or domains, turn on step 4 **Option s** and follow the instructions in the dialog box.
11. Click **Add Setting** when you are done.

> This rule can take up to 30 minutes to take affect and begin sending messages sent to the Archive Mailbox. Added or edited settings display highlighted in yellow-orange on the **Email** settings page.

Enable IMAP/POP in Google Apps

Use the following steps to enable IMAP/POP in the Archive Mailbox Settings.

1. Sign in to the Google Apps administrator control panel as the Administrator.
2. From the menu at the top of the page, select **Settings**.
3. From the left-navigation menu, click **Email**, and click **General Settings**.
4. Scroll down to **POP and IMAP access**, and clear the check box for **Disable POP and IMAP access for all users** to enable IMAP/POP.
5. Click **Save changes.**

>

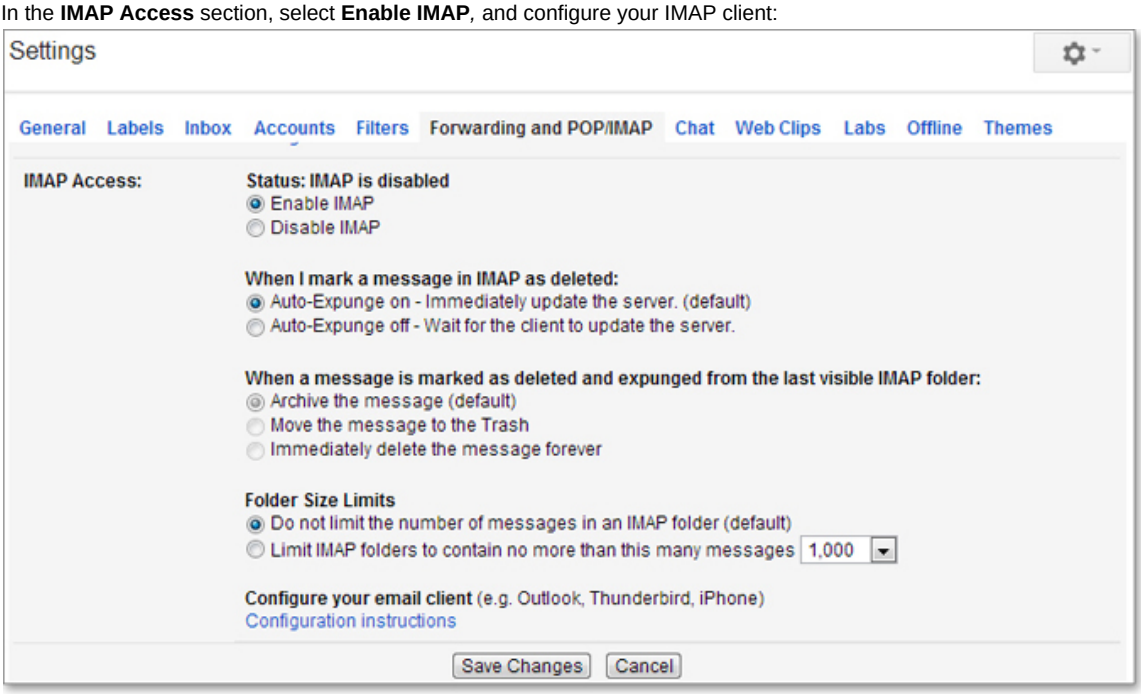
It can take 15-30 minutes for global IMAP and POP changes to take effect.

Enable IMAP/POP in Gmail

Each user must enable IMAP/POP in the Gmail settings under **Forwarding and POP/IMAP**.

To enable IMAP in Gmail:

1. Sign in to Gmail.
2. Click the **gear icon** in the upper right, then select **Settings**.
3. Click **Forwarding and POP/IMAP** at the top of the page.
4. In the **IMAP Access** section, select **Enable IMAP**, and configure your IMAP client:


Settings
General
Labels
Inbox
Accounts
Filters
Forwarding and POP/IMAP
Chat
Web Clips
Labs
Offline
Themes
IMAP Access:
Status: IMAP is disabled
Enable IMAP
Disable IMAP
When I mark a message in IMAP as deleted:
Auto-Expunge on - Immediately update the server. (default)
Auto-Expunge off - Wait for the client to update the server.
When a message is marked as deleted and expunged from the last visible IMAP folder:
Archive the message (default)
Move the message to the Trash
Immediately delete the message forever
Folder Size Limits
Do not limit the number of messages in an IMAP folder (default)
Limit IMAP folders to contain no more than this many messages
1,000
Configure your email client (e.g. Outlook, Thunderbird, iPhone)
Configuration instructions
Save Changes
Cancel

5. Click **Save Changes**.

In Gmail it is not possible to enable IMAP while using the basic HTML interface. You must use the standard view to see this option.

To enable POP in Gmail:

1. Sign in to Gmail.
2. Click the **gear icon** in the upper right, then select *Settings*.
3. Click **Forwarding and POP/IMAP** at the top of the page.
4. In the **POP Download** section, select **Enable POP for all mail** or **Enable POP for mail that arrives from now on**.
5. Choose what to do with your messages after your POP client or device receives them.
6. Configure your POP client, and then click **Save Changes**.

Add the Journal Account to the Barracuda Message Archiver

Once you configure the Service on Google Apps, you can add the journal account to the Barracuda Message Archiver to begin retrieving new messages for archiving.

1. Log in to the Barracuda Message Archiver as the administrator, and go to **MAIL SOURCES > Journal Accounts**.
2. In the **Journal Accounts** section, enter the following details:
   - **Enable Journal Accounts** – Select **Yes** to allow the Barracuda Message Archiver to poll the listed accounts for new messages for archiving.
   - **Enable Journal** – When set to **Yes**, all listed accounts are tested for connectivity with each page view**.**
   - **Polling Frequency** – Specify how often to poll each journal account for new messages.
3. In the **Journal Accounts Configuration** section, specify the following details for each journal account:
   - **Status** – Displays the connection status for each account.

- **Server** – Enter the Google Apps hostname.
- **Protocol** – Select whether the account is POP3 or IMAP; once you select the protocol, the default port number automatically populates the **Port** field.
- **Username** – Enter the "journaling" email address you created in the section Create an Archive/Journal Mailbox at the beginning of this article.
- **Password** – Enter the password associated with the email address.
- **Encryption** – Select the type of encryption used to connect to the mail server:
  - **TLS (if available)**
  - **TLS**
  - **SSL**
  - **None**
- **Port** – Select the associated port based on the selected protocol; the default value is port 143 for **IMAP**, and port 110 for **POP3**.

4. **Keep Items on Server**:
   - Select **Off** to allow the Barracuda Message Archiver to automatically clean up the contents of the journal mailbox after each import.
   - Select **On** to prevent the Barracuda Message Archiver from removing the journaled messages from Google Apps; *only* turn this option on if the contents of the journal account is required by other applications. In this case, make sure that another method for cleaning up the journal account is enabled on Google Apps in order to prevent unlimited growth on the mail server and to stay in compliance with your organization's message retention policies.

   > Barracuda Networks recommends that you set the value of **Keep Items on Server** to **Off** to save hard drive space on your mail server.

5. Click **Add** to add the journal account; verify the **Status** field displays green, and then click **Save Changes**.
6. To remove a journal account, click the **Delete** ( ) icon, and confirm you want to remove the account.

Barracuda Cloud Relay Service Configuration for Google Apps Mail Service

> This article refers to Barracuda Message Archiver firmware version 3.2 and higher, and applies to Google® Apps Business™ and Google Apps Education™ editions.

For customers using Google Apps Email service, it is possible to use the Barracuda Cloud Relay to relay journal mail from Google Apps Email to the Barracuda Message Archiver. Mail being journaled for Compliance purposes on Google Apps will be sent to the Barracuda Cloud Relay Service on port 25. The Barracuda Cloud Relay Service then sends the mail to your Barracuda Message Archiver on port 2500; you will need to open port 2500 on your corporate firewall.

> **Custom Token**
> Before completing the steps in this deployment, contact Barracuda Networks Technical Support and request a custom token to configure Barracuda Cloud Relay Service for Google Apps Mail Service.

Configure the Barracuda Message Archiver

Use the following steps to configure the Barracuda Message Archiver to accept mail on port 2500:

1. Log in to the Barracuda Message Archiver, and go to the **MAIL SOURCES > SMTP/IM** page.
2. In the **Enable SMTP/IM Forwarding**, enter **2500** in the **Additional Listening Ports** field. Click **Add**:

SMTP/IM Forwarding Settings
Save Changes
Help
Enable SMTP/IM Forwarding:
Yes
No
Whether this Barracuda Message Archiver accepts direct forwarding of messages. Recommended: Yes
Allow Only Trusted Hosts:
Yes
No
If enabled, then only hosts listed here will be able to forward messages to the Barracuda Message Archiver. Recommended: No
Additional Listening Ports
Add
2500
Non-standard ports over which the Barracuda Message Archiver will accept forwarded messages.

3. Click **Save Changes**.

To restrict the IP address from which the Barracuda Message Archiver accepts mail, contact Barracuda Networks Technical Support.

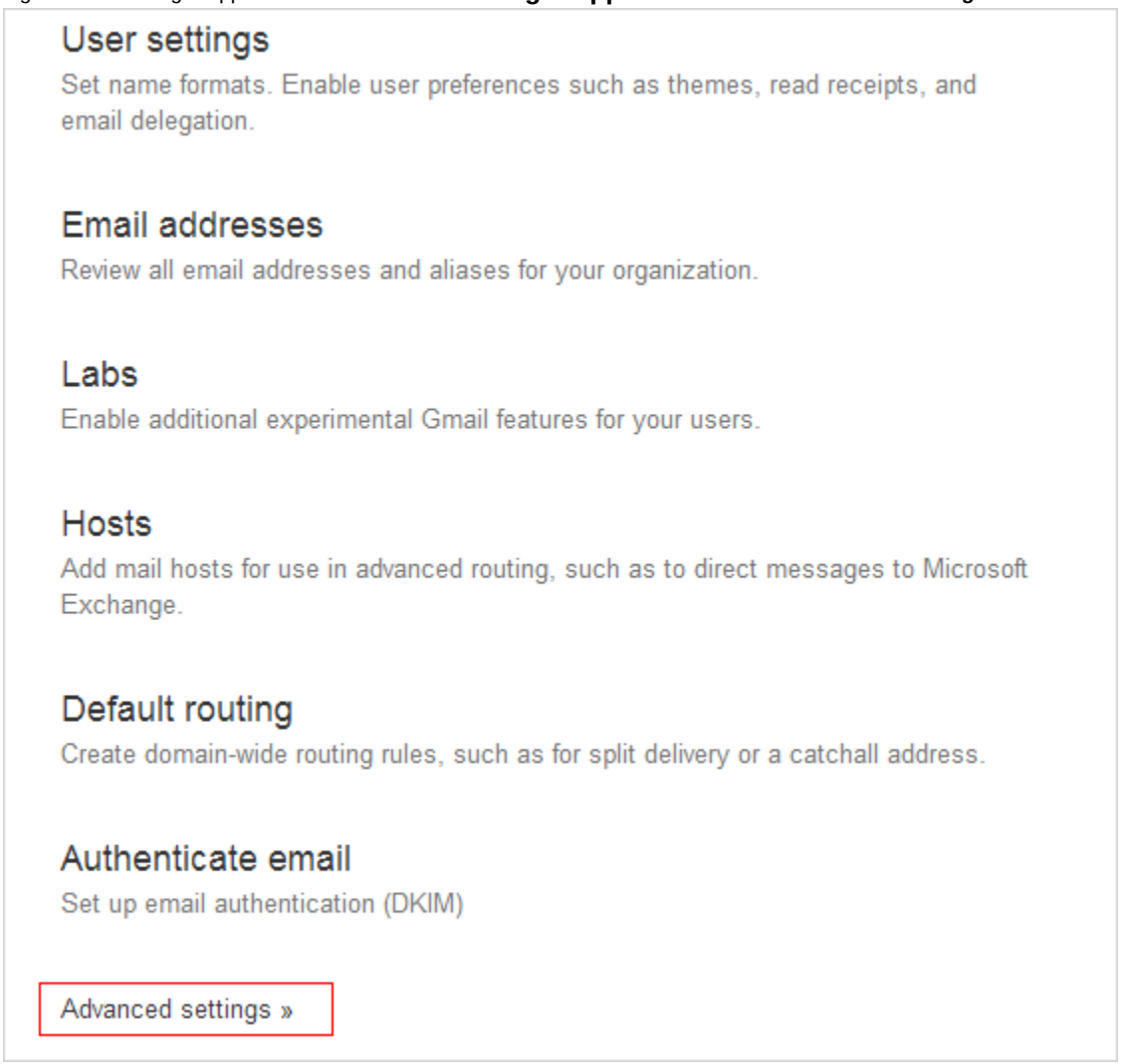
Configure Google Apps

Use the following steps to configure Google Apps to send journal mail to Barracuda Networks Cloud Relay:

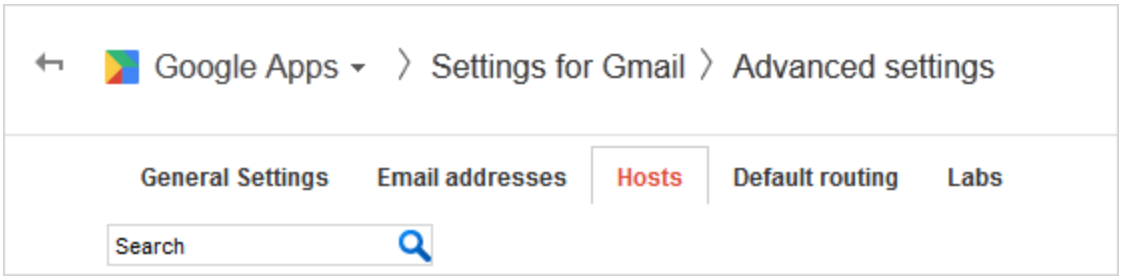
Custom Token
You must have your custom token from Barracuda Networks Technical Support to configure Barracuda Cloud Relay Service for Google Apps Mail Service.

Please note: The Barracuda Cloud Relay Service cannot accept your journal mail traffic until Barracuda Support indicates that the Relay Service has been configured for your account.

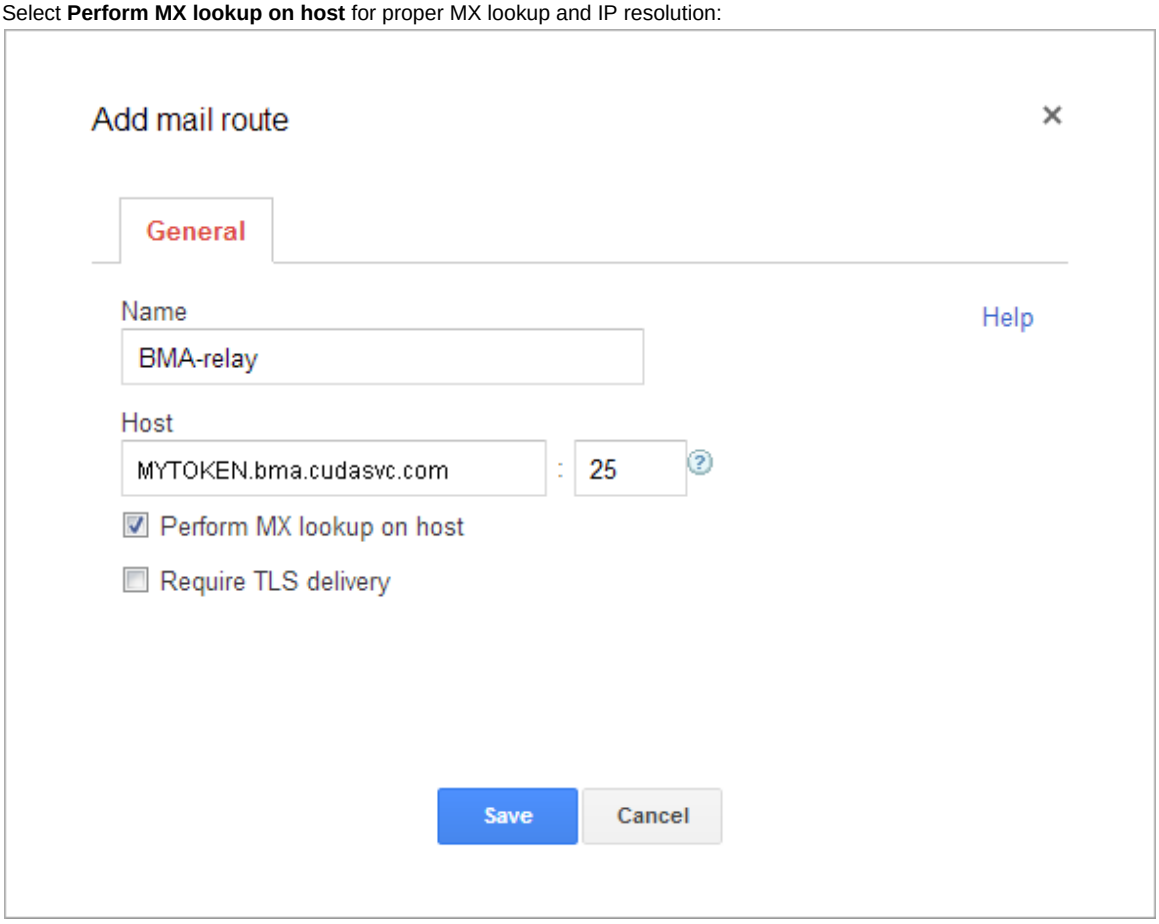
1. Log in to your Google Apps, and click **Sign in**. Enter your domain name, select **Domain management** from the drop-down menu, and click **Go**.
2. Sign in to the Google Apps domain console. Click **Google Apps > Gmail > Advanced settings**:


User settings
Set name formats. Enable user preferences such as themes, read receipts, and email delegation.
Email addresses
Review all email addresses and aliases for your organization.
Labs
Enable additional experimental Gmail features for your users.
Hosts
Add mail hosts for use in advanced routing, such as to direct messages to Microsoft Exchange.
Default routing
Create domain-wide routing rules, such as for split delivery or a catchall address.
Authenticate email
Set up email authentication (DKIM)
Advanced settings »

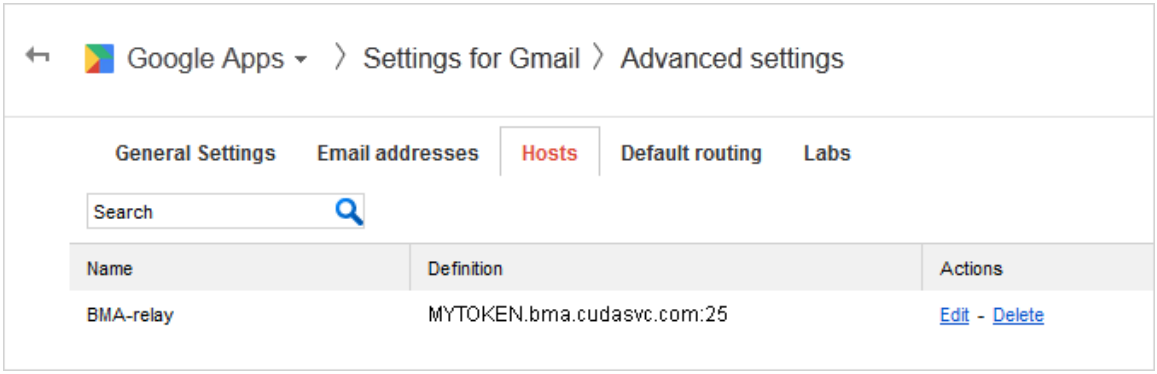
3. In the **Advanced settings** window, click the **Hosts** tab:



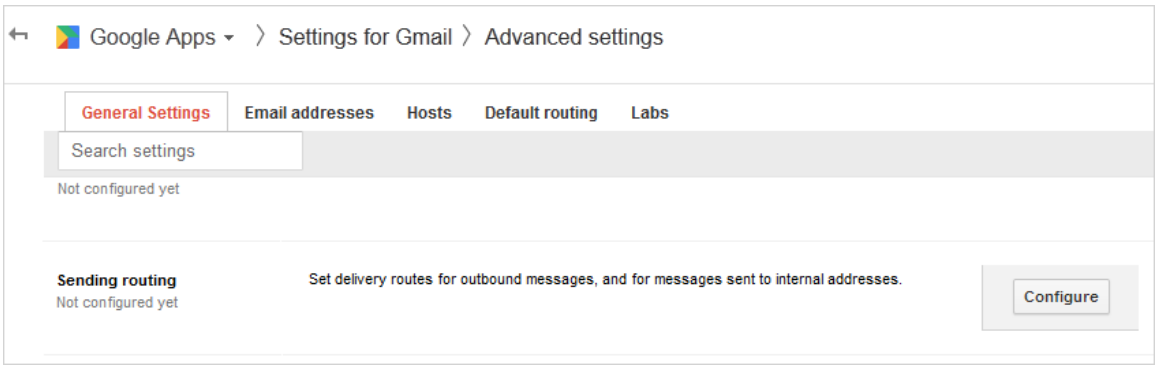
4. Click **Add route**. In the **Add mail route** window, type `BMA-relay` in the **Name** field, and e nter the host name provided to you by Barracuda Networks Technical Support including your custom token. For example, *mytoken*.bma.cudasvc.com
5. Select **Perform MX lookup on host** for proper MX lookup and IP resolution:



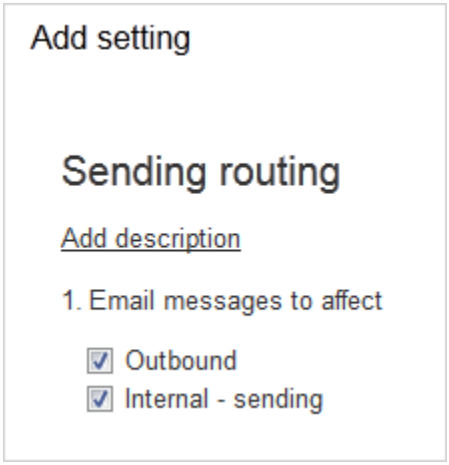
6. Click **Save**. Your entry displays in the **Hosts** list:



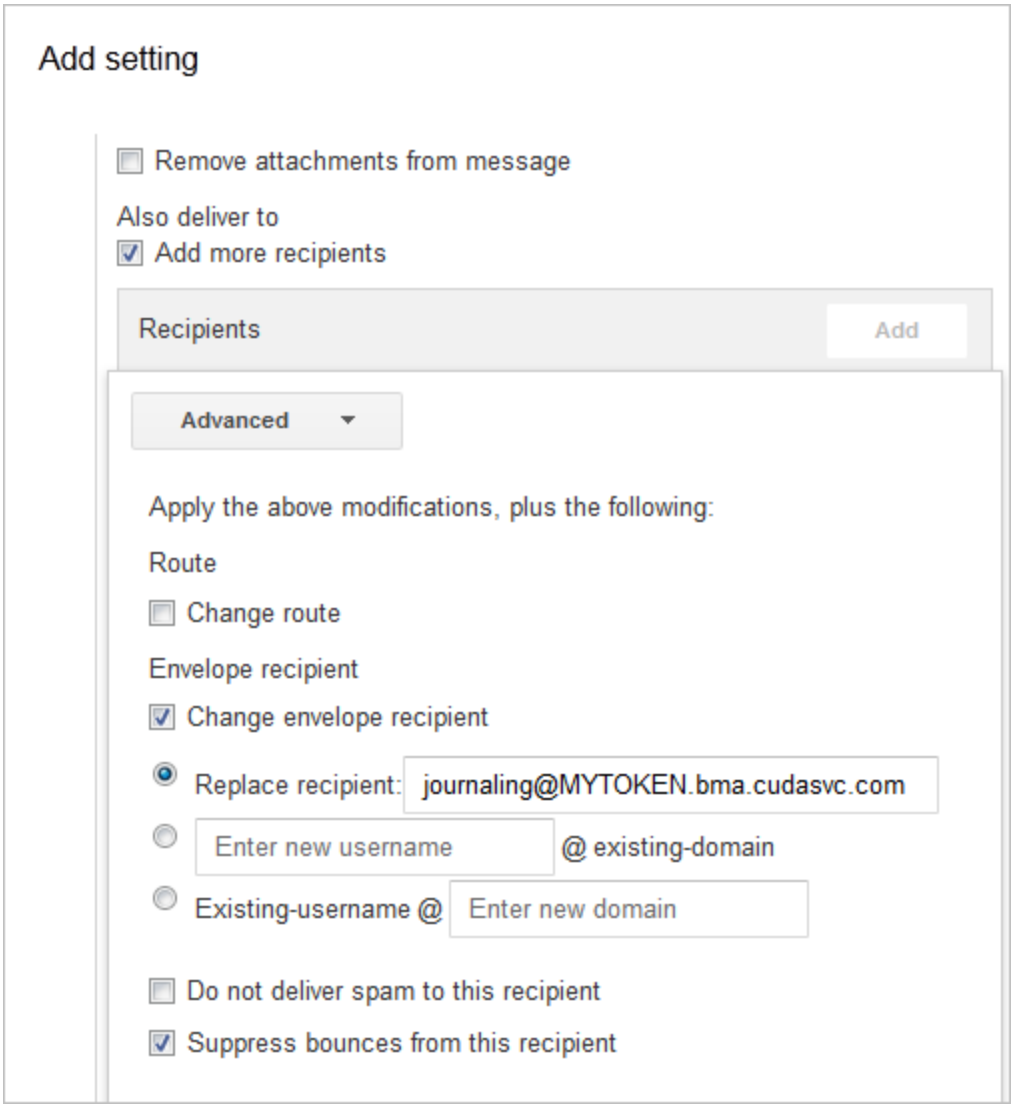
7. Click the **General Settings** tab, scroll down to **Sending routing**, and click **Configure**:



8. In the **Email messages to affect**, select **Outbound** and **Internal - sending**:

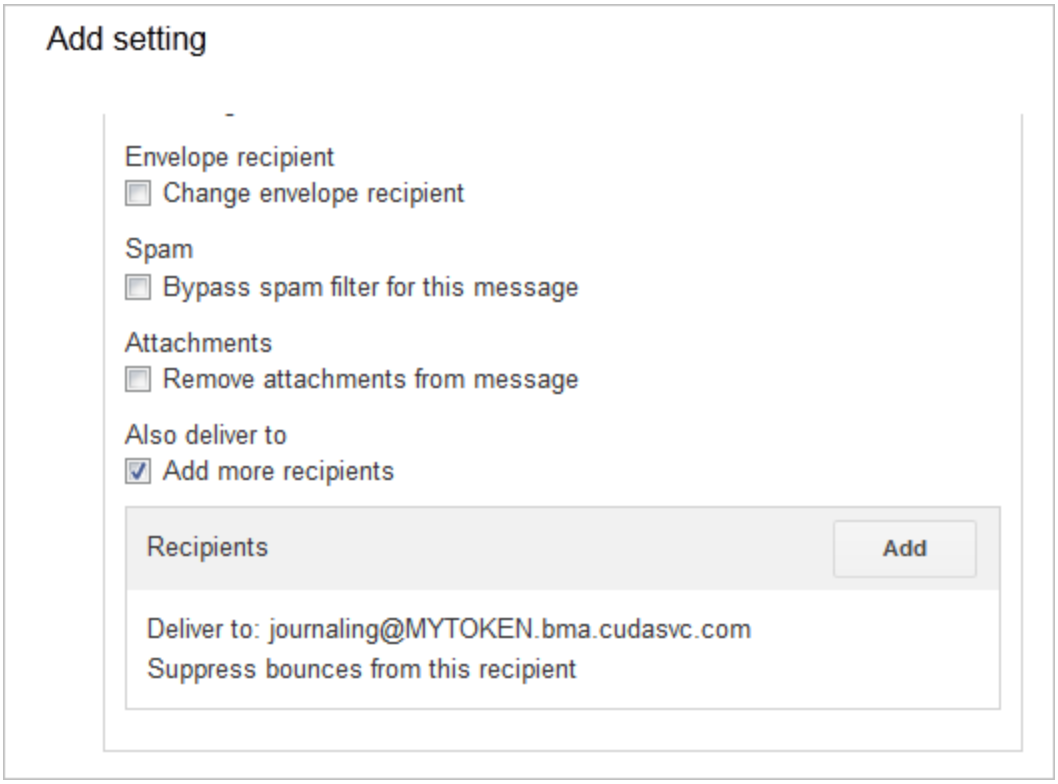


9. Scroll down to **Also deliver to**, and select **Add more recipients**. In the **Recipients** setting, select **Advanced** from the drop-down menu, and select **Change envelope recipient**.
10. In the **Replace recipient** field, enter `journaling@` followed by the host name provided to you by Barracuda Networks Technical Support including your custom token, as the recipient. For example, `journaling@mytoken.bma.cudasvc.com`
11. Select **Suppress bounces from this recipient**:

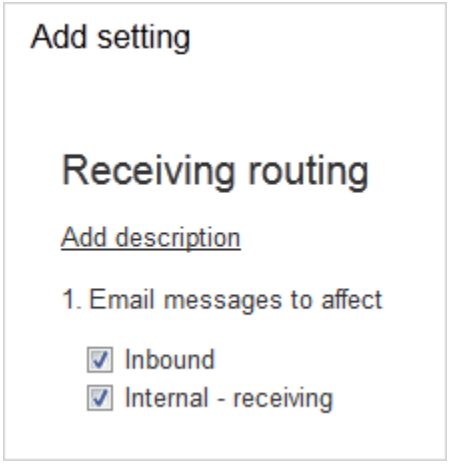


Spam Filtering
You can optionally select **Do not deliver spam to this recipient**. However, if you select this option and you spam filter journal mail, the Barracuda Message Archvier will not receive any email that Google Apps considers to be spam.

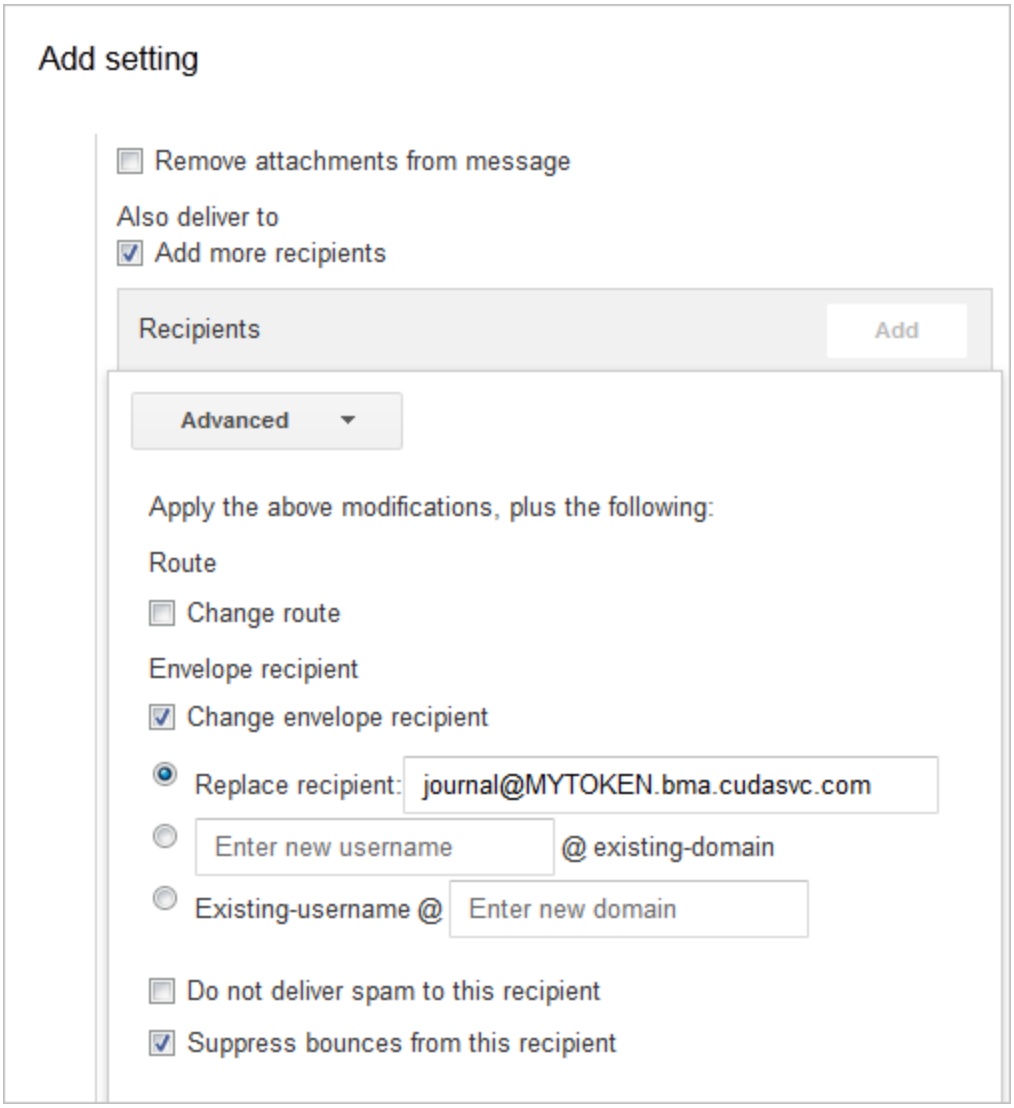
12. Scroll down and verify the settings; click **Add**:



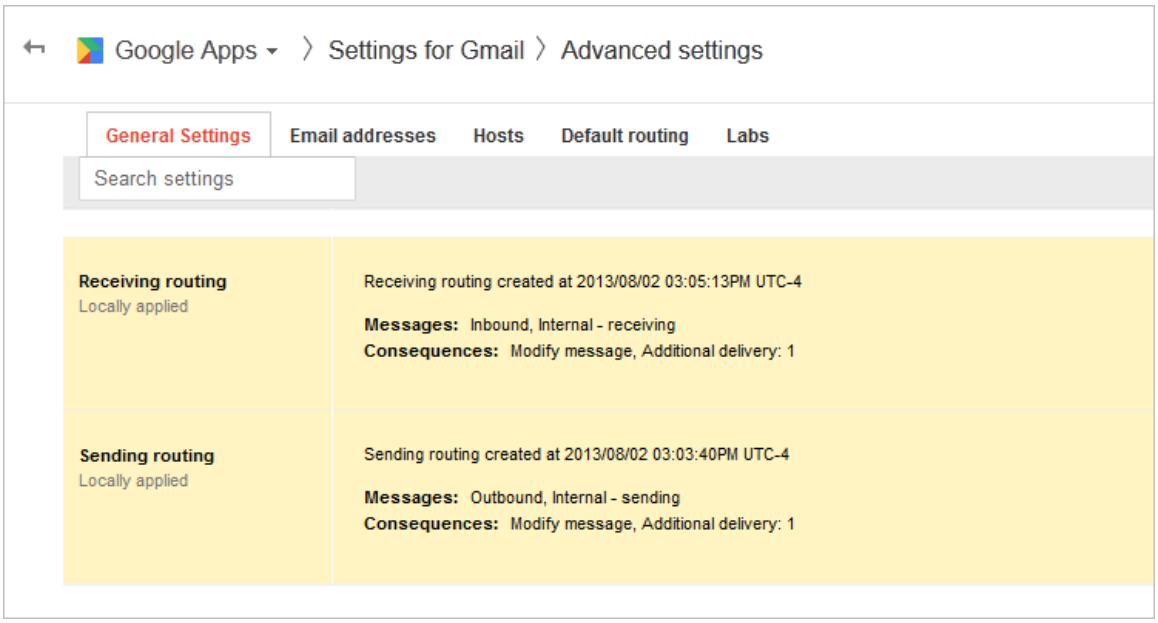
13. In the **General Settings** tab, scroll down to **Receiving routing**, and click **Configure**.
14. In the **Email messages to affect**, select **Inbound** and **Internal - receiving**:



15. Scroll down to **Also deliver to**, and select **Add more recipients**. In the **Recipients** setting, select **Advanced** from the drop-down menu, and select **Change envelope recipient**.
16. In the **Replace recipient** field, enter `journaling@` followed by the host name provided to you by Barracuda Networks Technical Support including your custom token, for example, `journal@mytoken.bma.cudasvc.com`.
17. Turn on **Suppress bounces from this recipient**:



18. Scroll down and verify the settings; click **Add**.
19. The **Receiving routing** and **Sending routing** options display in the **General Settings** page:



Supplemental Service Information

GroupWise Deployment

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher, and Novell® GroupWise® 6.5 and higher, except where noted.

In this article:

- Trusted Application Key Options
  - Option 1. Download the Trusted Application Key Generator
  - Option 2. Manually Generate a Trusted Application Key
  - Option 3. Create a Trusted Application Key on GroupWise 8 Support Pack 1 and Higher
- Import GroupWise Messages
- Troubleshoot GroupWise Mail Archiving
  - Additional GroupWise Troubleshooting Resources

Related Articles

- Importing GroupWise Messages
- GroupWise Trusted Application Keys
- Create GroupWise Trusted Application Key

Additional Resource

- Novell GroupWise website
- Resolving GWCheck Problems
- Mobile Email Sync with Novell Data Synchronizer
- How to fix GroupWise mailbox system folders

To archive messages from Novell GroupWise Servers to the Barracuda Message Archiver, the following must be true for each GroupWise Server:

- The Barracuda Message Archiver has been added as a Trusted Application within Groupwise;

  For more information, see Trusted Applications on the Novell website.
- Message Retention is enabled;
- Each Server has a GroupWise Trusted Application Certificate; and
- The Server user mailboxes are healthy and provide mail to the Barracuda Message Archiver when access is requested.

Additionally, once a Trusted Application Key is in place, to automatically populate the GroupWise username list section of the Barracuda Message Archiver web interface, you must have Simple Object Access Protocol (SOAP) enabled on the Post Office to which you want to connect.

A Trusted Application Key allows the Barracuda Message Archiver to access user mailboxes as a "super user" and allows them to access the account without requiring a user password. See the section **Trusted Application Key Options** below for details.

The Trusted Application Key provides access to every account in the GroupWise system. You can secure the Trusted Application Key from unauthorized use by specifying a retention flag against the Trusted Application Key in combination with the IP address of your Barracuda Message Archiver. See the Novell GroupWise website for details on working with Trusted Application Keys and creating retention flags.

When Retention is enabled on the GroupWise Server, end-users cannot delete emails from their mailbox until all emails present in the mailbox have been marked by GroupWise as having been read by the Barracuda Message Archiver.

Trusted Application Key Options

Select the manner in which you want to create a Trusted Application Key:

- Option 1. Download the Trusted Application Key Generator from the **USERS > Client Downloads** page in the Barracuda Message Archiver to generate the GroupWise Trusted Key.
- Option 2. Manually Generate a Trusted Application Key.
- Option 3. Create a Trusted Application and its associated Key in ConsoleOne®; available in GroupWise 8 Support Pack 1 or higher *only*.

Option 1. Download the Trusted Application Key Generator

Click here to expand...

Use the following steps to generate a GroupWise Trusted Key:

1. Log into the Barracuda Message Archiver web interface, and go to the **USERS > Client Downloads** page.
2. Download the **Trusted Application Key Generator** to a workstation that has the GroupWise client, the Novell 32-bit client installed, and is logged into the same eDirectory tree as the GroupWise Server.
3. From that workstation, execute the downloaded Key Generator to create a Trusted Application Key to be uploaded onto the Barracuda Message Archiver; you must know the location of the domain directory.
4. Go to the section **Import GroupWise Messages** to import Novell GroupWise messages into the Barracuda Message Archiver.

Option 2. Manually Generate a Trusted Application Key

Click here to expand...

A Trusted Application Key is created at the Domain database level. To create this key, you need the following:

- An application capable of creating the Trusted Application Key such as the GroupWise Trusted App Key Maker available on the **USERS > Client Downloads** page of the Barracuda Message Archiver

  > **Novell GroupWise 8 Support Pack 1 and Higher**
  > Starting with GroupWise 8 Support Pack 1, you can create a trusted application and its associated key in ConsoleOne for use with the Barracuda Message Archiver. For more information, refer to **Option 3** below.

- Administrator access to the GroupWise wpdomain.db database
- Administrator privileges to the Domain object within eDirectory

For step-by-step instructions, refer to How to Create a GroupWise Trusted Application Key.

Go to the section **Import GroupWise Messages** to import Novell GroupWise messages into the Barracuda Message Archiver.

Option 3. Create a Trusted Application Key on GroupWise 8 Support Pack 1 and Higher

Click here to expand...

> **GroupWise 8 Support Pack Version 1 and Higher Only**
> This option applies only to Novell GroupWise 8 Support Pack 1 and higher.

Starting with GroupWise 8 Support Pack 1, you can create a trusted application and its associated key in ConsoleOne for use with the Barracuda Message Archiver.

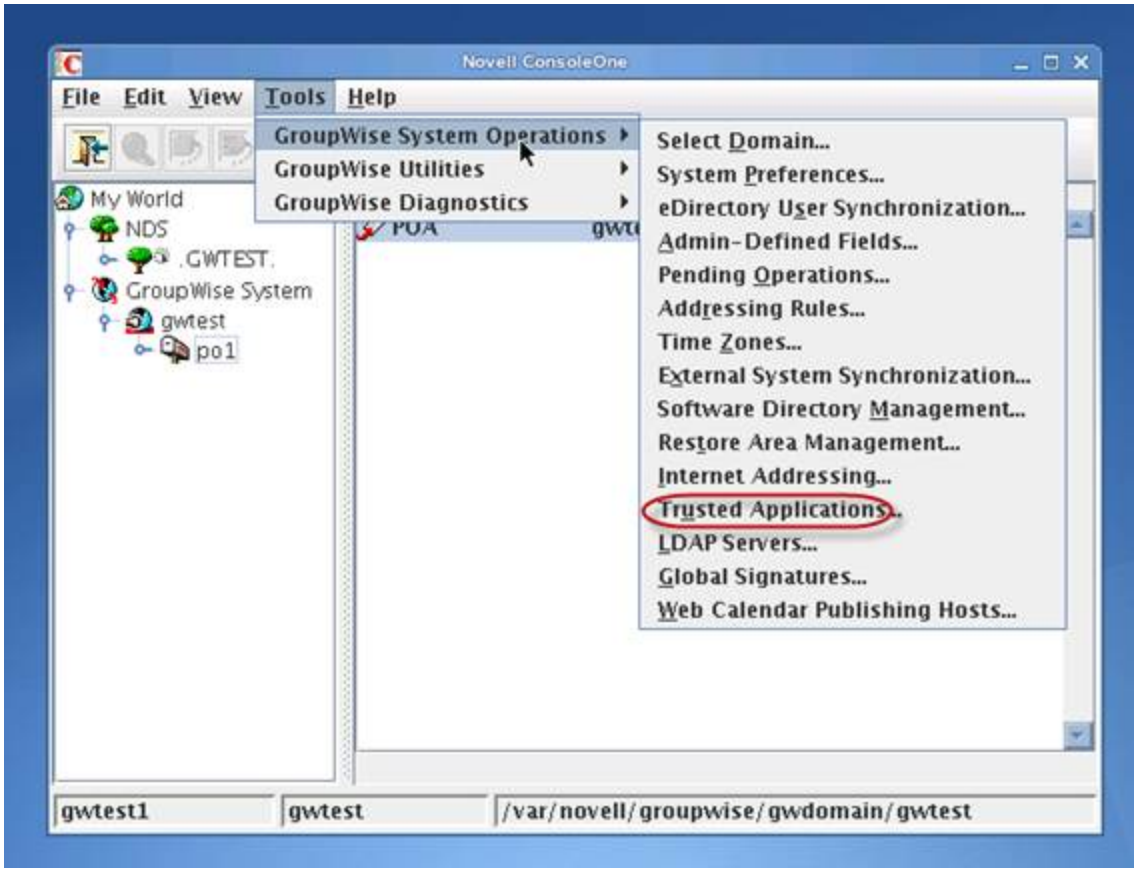
Message Retention Support

In order for GroupWise mailboxes to support message retention, complete the following steps:

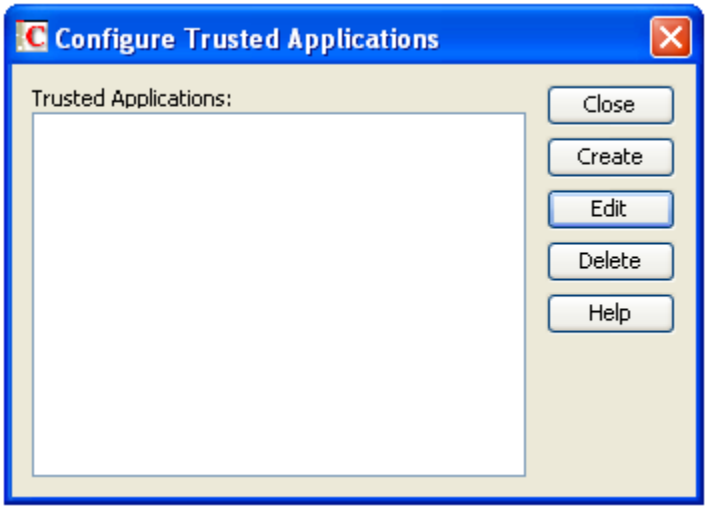
1. Open Novell ConsoleOne, and go to **Tools > GroupWise Utilities > Client Options > Environment > Retention**.
2. In the dialog, select the retention options:
   - **User** – Enable individual mailboxes
   - **Post Office** – Enable all mailboxes in a post office
   - **Domain** – Enable all mailboxes in a domain
3. Click **OK** to save your settings.

Set Up Trusted Application

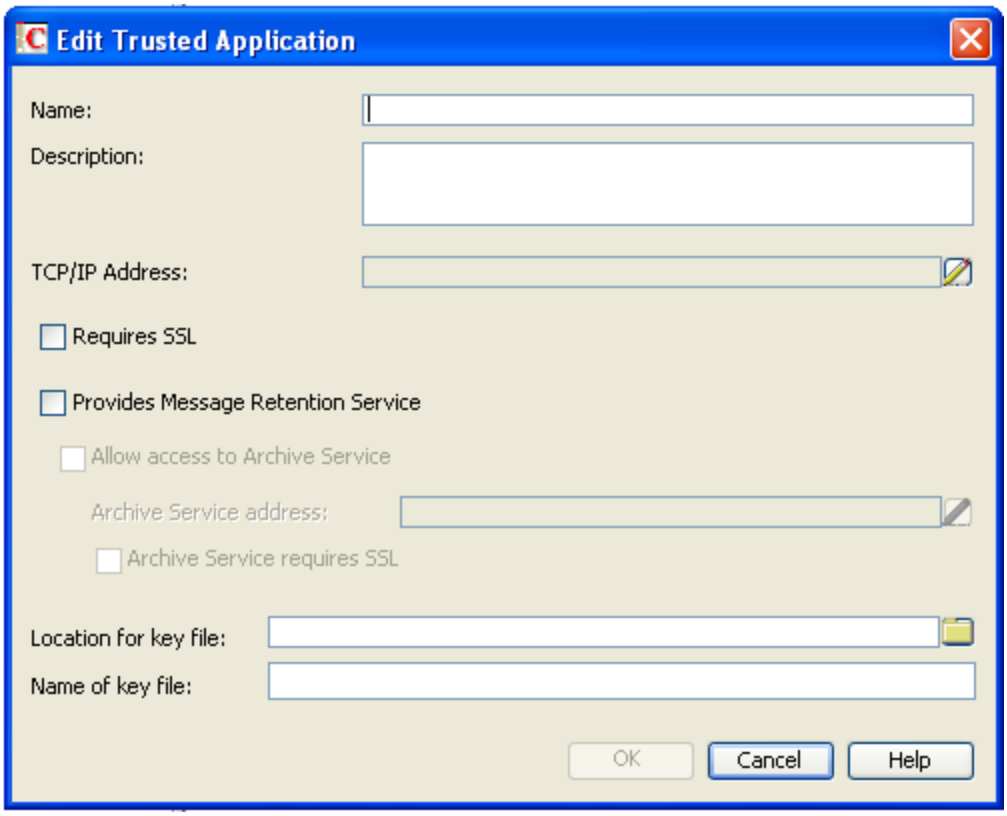
1. Open Novell ConsoleOne, and go to **Tools > GroupWise System Operations > Trusted Applications**:



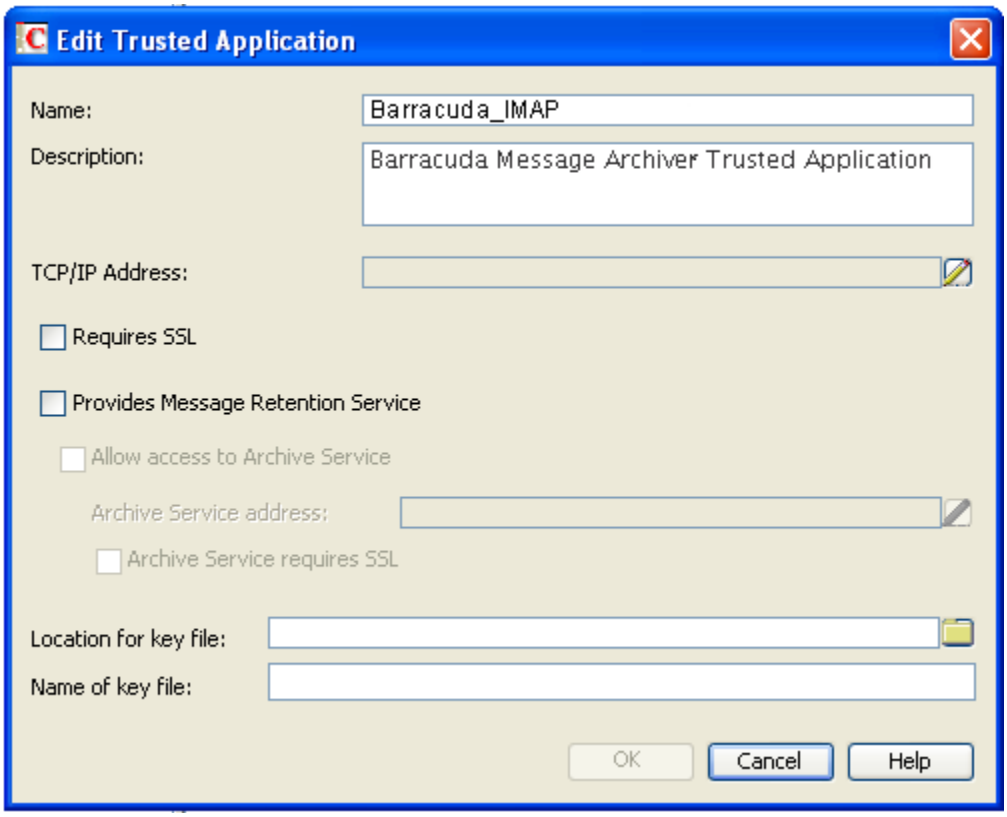
2. In the **Configure Trusted Applications** dialog box, click **Create:**



3. The **Edit Trusted Application** dialog box displays:



4. In the **Edit Trusted Application** dialog box, enter *Barracuda_IMAP as* the trusted application name in the **Name** field.
5. In the **Description** field, enter a description for the trusted application:



6. **TCP/IP Address** field:
   - To allow the trusted application from any server, leave this field blank.
   - To restrict the location from which the trusted application can run, click the **Edit** icon next to the field, and specify the IP address or DNS hostname of the trusted application server.
7. To require a secure (SSL) connection between the trusted application, post office agents (POAs), and Internet Agents, turn on **Requi**

res SSL.

8. If the purpose of the trusted application is to retain GroupWise user messages by copying them from GroupWise mailboxes into another storage medium, select **Provides Message Retention Service**.
9. Select **Allow Access to Archive Service** to allow message retention to interact with the Barracuda Message Archiver.
10. The following options are not applicable for configuration with the Barracuda Message Archiver*:*
    - **Archive Service Address** – leave this field blank.
    - **Archive Service Requires SSL** – deselect.
11. Click the **Browse** icon to the right of the **Location for key file** field, and browse to and select the directory where you want to create the trusted application key file.
12. In the **Name of Key File** field, enter the trusted application key file name.
13. Click **OK** to save the trusted application configuration information.
14. Go to the section **Import GroupWise Messages** to import Novell GroupWise messages into the Barracuda Message Archiver.

Import GroupWise Messages

Use the following steps to enable archiving with Novell GroupWise:

1. Log in to the Barracuda Message Archiver web interface, and navigate to the **MAIL SOURCES > GroupWise Sync** page.
2. Configure the items in the **GroupWise Synchronization** section for each GroupWise server. Enter the key in the **Trusted Application Key** field.
3. Select the desired method for populating the list of users you want to retrieve email:
    - Click **Populate** to automatically retrieve users from the server, *or*
    - Manually enter the user names in the **Username List** field.
4. Save your changes to enable the Barracuda Message Archiver to maintain synchronicity with your GroupWise Server.

Troubleshoot GroupWise Mail Archiving

The Barracuda Message Archiver connects and authenticates to the GroupWise Mail Servers via the IMAP protocol using the GroupWise-documented Trusted Application Key access. This allows the Barracuda Message Archiver to retrieve emails from the GroupWise Server user mailboxes and mail folders. However, if there are issues with particular GroupWise user mailboxes or mail folders—permissions, file naming scheme, or even corruption—GroupWise is unable to present content to the Barracuda Message Archiver when the Barracuda Message Archiver requests data. These issues will often affect other IMAP clients as well.

One symptom of such issues with the GroupWise Mail Server is that an end-user is unable to empty their trash when **Empty trash** is clicked. This is a sign that the GroupWise Server recognizes that there is email in the user mailbox that *has not been archived*, and the GroupWise Server is thus protecting the content until archiving is successful. To achieve this level of protection, the GroupWise admin must have enabled the Message Retention flag feature on their GroupWise Server (see the Novell website). Once the issue on the GroupWise Server is resolved and the Barracuda Message Archiver is able to collect all mail from within a user mailbox, the end-user is again able to empty their trash folder.

> **Retention Time**
> For GroupWise retention time, the Barracuda Message Archiver sets the *digest* retention time; the *modified* retention time is not used or changed. However, GroupWise references the *modified* retention time to determine if a user is allowed to empty their trash. If a system administrator has manually set the *modified* retention time, or this value has been populated by a utility or application, the user may be unable to empty their trash until the *modified* retention time value is cleared for the mailbox.

Additional GroupWise Troubleshooting Resources

For additional information about troubleshooting issues with GroupWise Server mail boxes, the following Novell documentation may be useful:

- If there is an issue retrieving mail from a particular GroupWise Server user mailbox or mail folder, you can use the Novell utility **GWCHECK** which examines user mailboxes and mail folders, identifies issues, and suggests repair options. For details, refer to the Novell article GWCheck Problems
- For details on fixing GroupWise mailbox system folders, refer to the Novell support article How to fix GroupWise mailbox system folders
- Certain IMAP mail clients may set flags or properties on user mailboxes or folders that impact access by any other IMAP connection, including the Barracuda Message Archiver's TAPP key access. GroupWise customers experiencing issues of this type may want to consider switching their mobile and similar mail clients to use Novell Data Synchronizer. Use of the Data Synchronizer eliminates problems caused by competing IMAP sessions.

> - Barracuda Networks Technical Support is able to run diagnostic tools from the Barracuda Message Archiver that may help identify which GroupWise user mailboxes and mail folders are experiencing issues that can then be addressed by the GroupWise Administrator.

- If you continue to encounter GroupWise mail archiving issues after running the Novell tools, Barracuda Networks recommends that you contact Novell to resolve the issue.

Kerio Connect Mail Server Deployment

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher, and the Kerio Connect Mail Server.

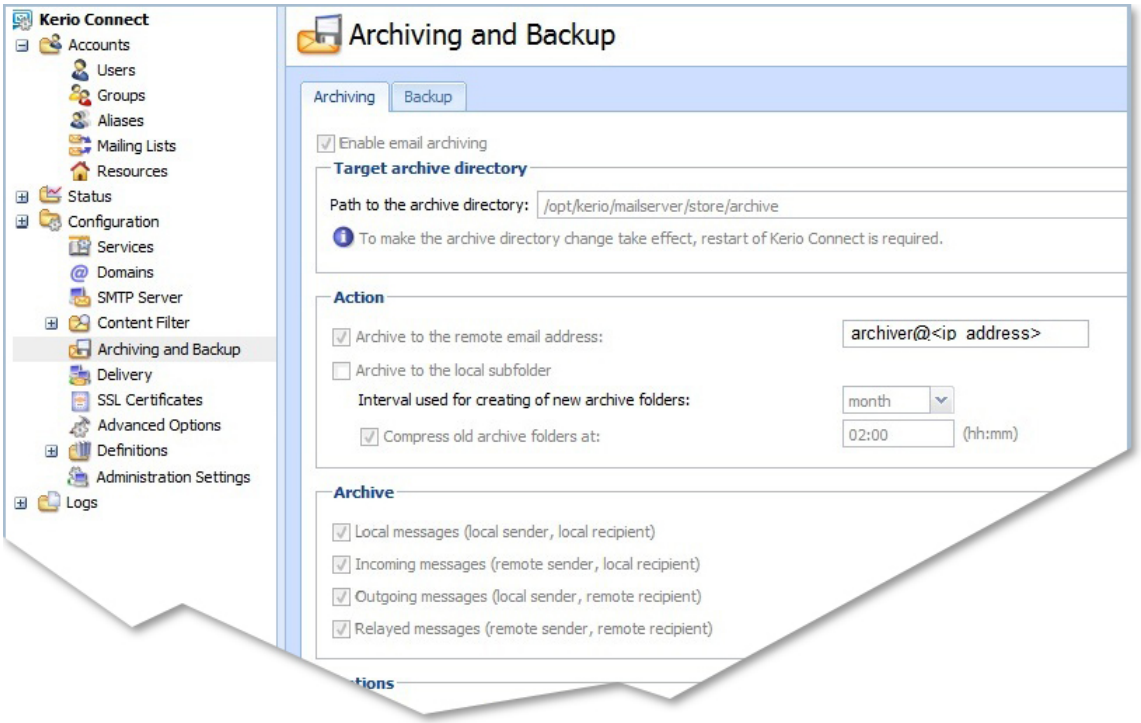
Related Articles

- Routing Outbound Mail through Barracuda Spam Firewall
- Message Import, Stubbing & Configuration

Use the following steps to configure Kerio Connect to send all messages to the Barracuda Message Archiver.

1. Navigate to the Kerio Connect directory, expand **Configuration**, and click **Archiving and Backup**.
2. In the **Archiving** tab, turn on **Enable email archiving** to facilitate archiving to the Barracuda Message Archiver. In the **Path to the archive directory** field, enter the full path to the archive directory based on the conventions of the operating system on which Kerio Connect is running.

   Important
   Do not use the UNC as the path specification.
3. In the **Actions** section, enter the remote email address in the **Archive to the remote email address** field, for example, `archiver@192.168.200.200`. Email is resent to this remote email address.
4. In the **Archive** section, select the following options:
   a. **Local messages (local sender, local recipient)** – All local messages (messages sent from the local domain) will be archived
   b. **Incoming messages (remote sender, local recipient)** – All incoming messages will be archived (from remote senders to local recipients)
   c. **Outgoing messages (local sender, remote recipient)** – All outgoing messages will be archived (from local senders to remote recipients)
   d. **Relayed messages (remote sender, remote recipient)** – All messages forwarded to a relay server will be archived (from remote senders to remote recipients)



Important
To archive all messages *before* the antivirus check begins, turn on **Archive messages before applying the content filter check**.

When enabled, all messages are stored intact; any viruses contained within the messages are stored in these files.

Once configured, an archive folder is automatically created when the first message is delivered. The folder is named based on the selected interval (daily, weekly, or monthly) in the **Archiving** tab. Any time Kerio Connect is restarted, a new archive folder is created upon receiving the first message, and uses the settings specified in the Archiving section in the **Archiving** tab.

IBM Lotus Notes/Domino IMAP Deployment

This article refers to the Barracuda Message Archiver firmware version 3.1 or higher, and IBM® Notes®/IBM Domino® 8.5 or later running on a Microsoft Windows-based system.

The IBM Notes/IBM Domino IMAP interface is designed to allow a user access to their mail file via the IMAP interface. In order to access the NSF file **mailjrn.nsf**, it is necessary to set **mailjrn.nsf** as the **BarracudaMailArchiver** user email database. Note that the Mail Archiver database template is based on the standard mail archive template and requires only a few changes to allow access via IMAP. There are two changes: the addition of folders expected by IMAP, and the addition of logic to copy all messages to the Inbox folder which IMAP reads.

In this article:

- Procedure
  - Step 1. Load the Journal/Application into IBM Domino Designer
  - Step 2. Create Agent
  - Step 3. Update the Mail File Value
  - Step 4. Set Privileges
- Test Your Settings

Related Articles

- How to Import IBM Notes NSF Files

Additional Resource

- Barracuda Networks Knowledgebase Solution #00006095

IBM Notes 9 Social Edition

In IBM Notes 9, the toolbar does not display by default except in edit mode. Use the following steps to toggle the toolbar so that you can access the Barracuda Message Archiver from the toolbar:

1. Open the IBM Notes Inbox.
2. From the **View** menu, point to **Toolbar**, and click **Show Toolbars Only When Editing** to toggle the option *off*.

The toolbar now displays in all modes. For additional information, refer to the infolib IBM Notes 9.0 Help content.

Important Notes

- Because the IBM Domino attachment and object service (DAOS) stores file attachments in a separate repository on the server that are retrieved by reference, before working with the NSF Import Utility, first restore these attachment objects to the customer mailbox.
- The maximum size email that can be retrieved by the Barracuda Message Archiver via POP or IMAP is 100MB.

Procedure

- The following steps describe how to configure IBM Notes/IBM Domino to use Mail Journaling on a local database. The steps use the file name **mailjrn.nsf**; substitute the actual file name when completing the configuration.
- The following steps describe how to configure an IBM Notes/IBM Domino account specifically for the Barracuda Message

Archiver to allow connection to IBM Notes/IBM Domino use the account name **BarracudaMailArchiver**; substitute the actual file name when competing this configuration.

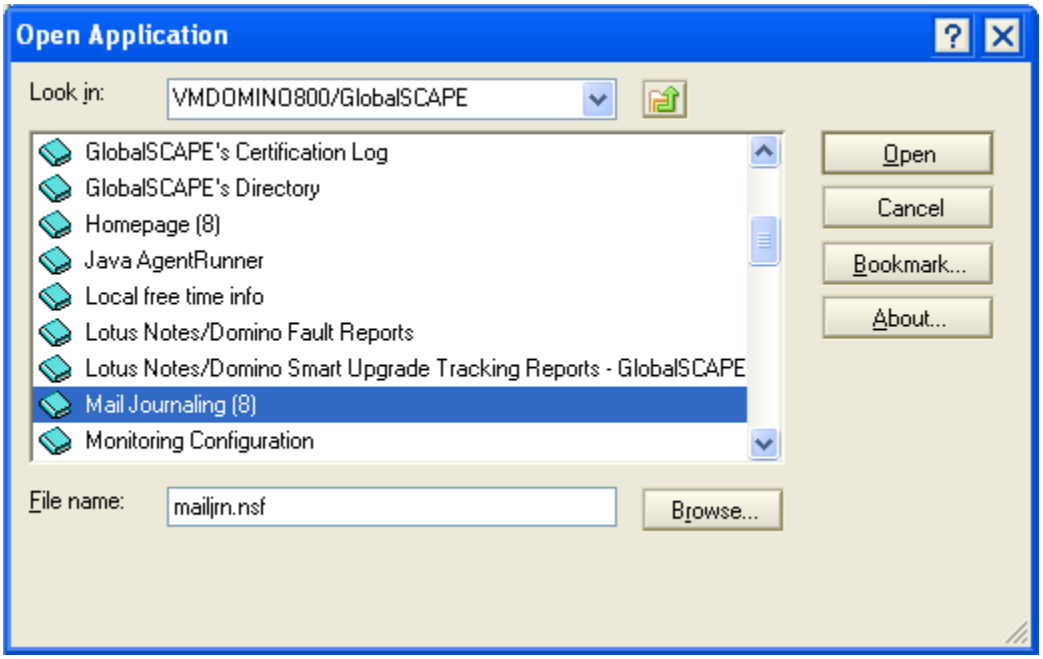
Log in to the IBM Notes Client Console, and verify Journaling is capturing emails and that the journal file **mailjrn.nsf** can be opened from the **Barracuda MailArchiver** account. If IMAP is not enabled, run the following command from the IBM Notes Client Console to enable IMAP on the Journal file **mailjrn.nsf**:

```
load convert -e mailjrn.nsf
```

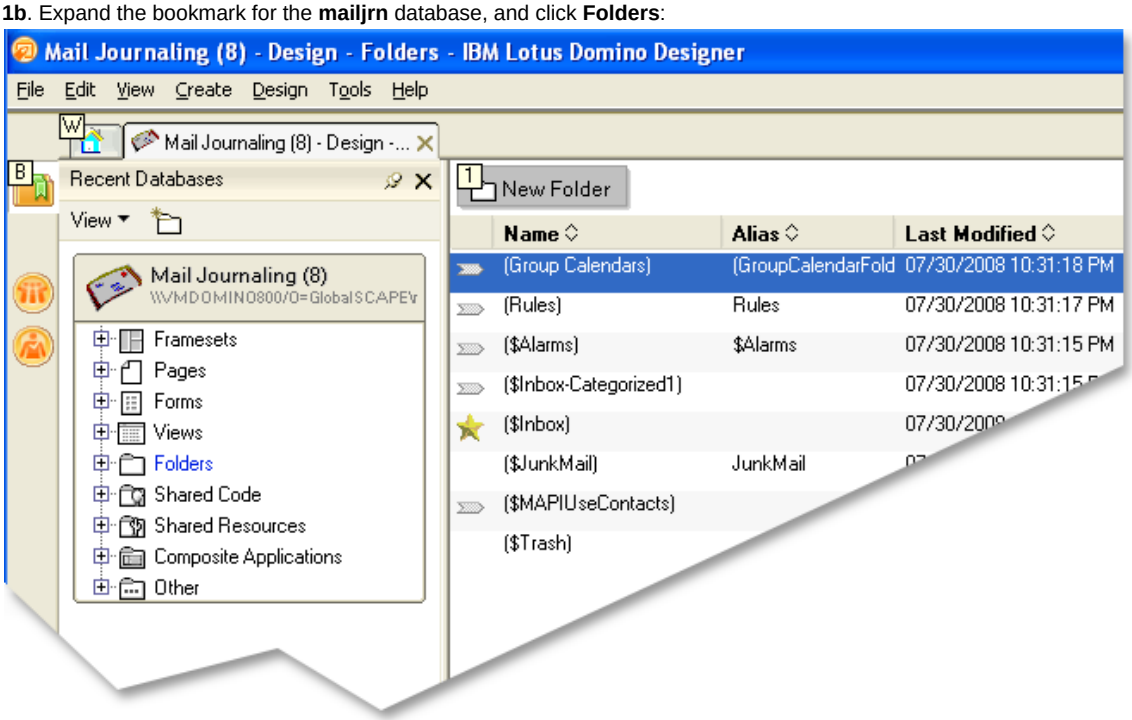
Step 1. Load the Journal/Application into IBM Domino Designer

Use the following steps to load the journal database/application into IBM Domino Designer.

1a. Log in to IBM Domino Designer, and click **Open Application**:

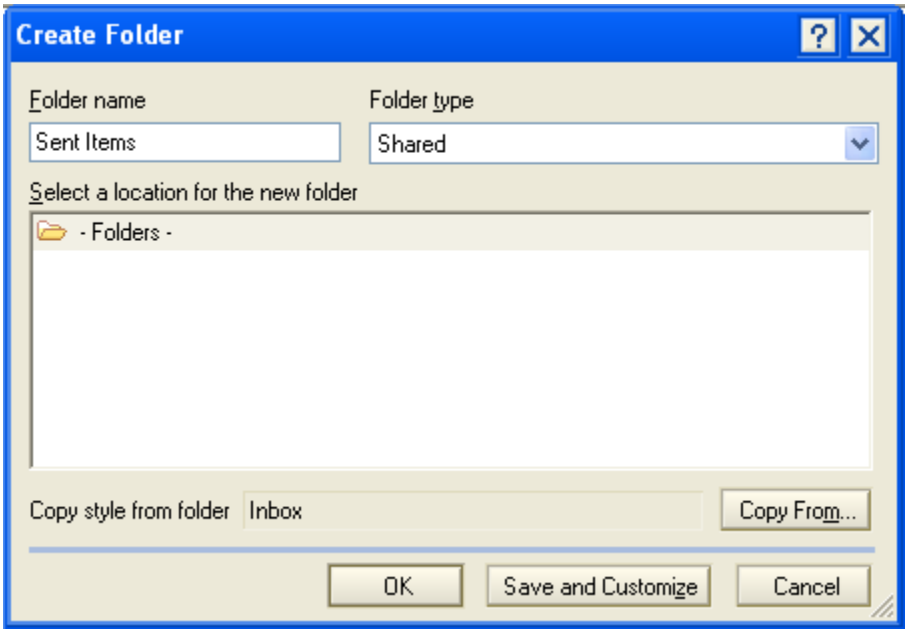


1b. Expand the bookmark for the **mailjrn** database, and click **Folders**:



1c. IMAP requires the presence of the **Sent Items** and **Drafts** folders. If these folders are present, go to **Step 2. Create Agent**. If they are not present, complete steps 1d and 1e.

1d. Click **New Folder**, and in the **Create Folder** dialog box, enter **Sent Items** in the **Folder name** field:

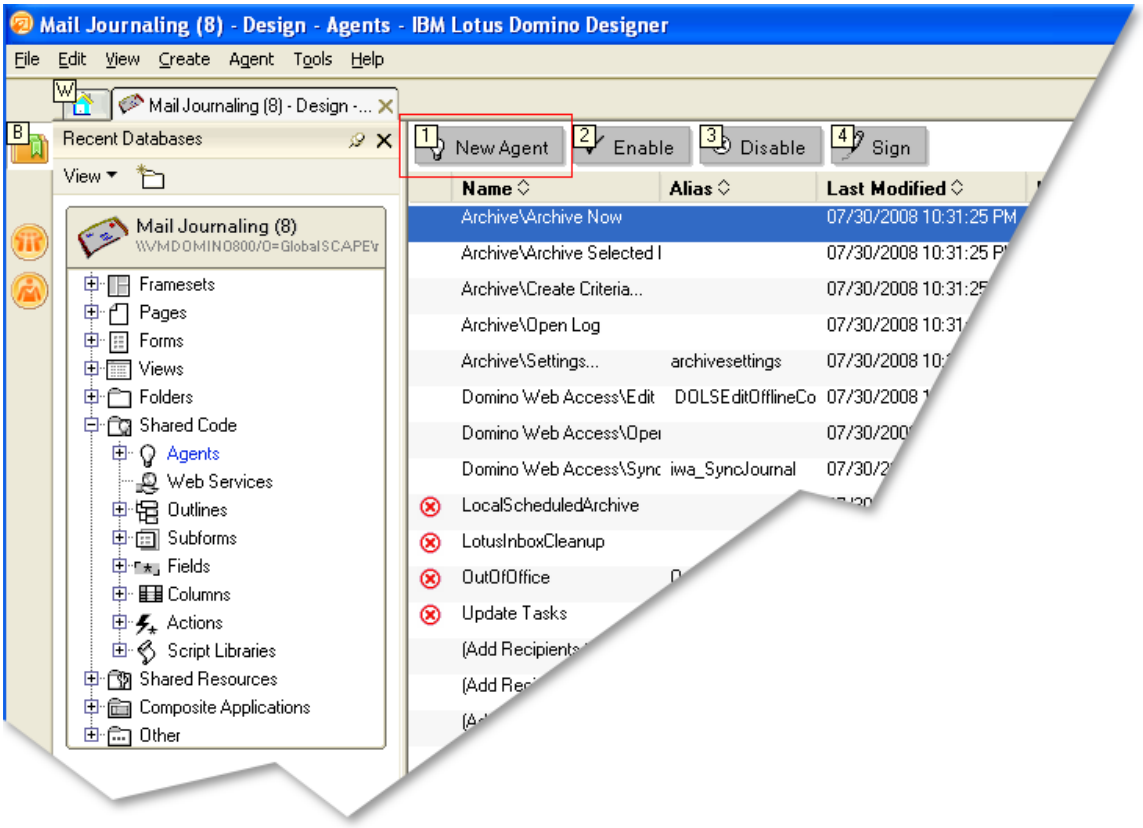


1e. Click **OK**. The **Sent Items** folder is added. Click **New Folder**, and in the **Create Folder** dialog box, type `Drafts`. Click **OK** to add the folder.

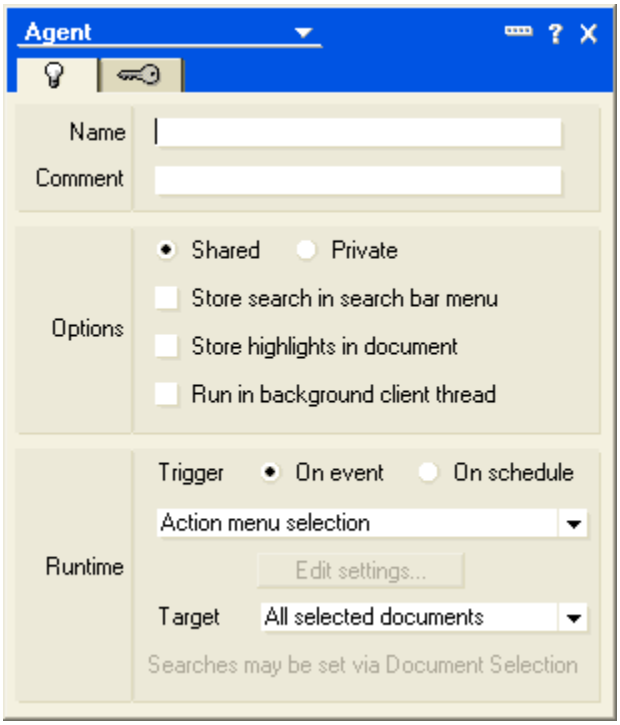
Step 2. Create Agent

Use the following steps to create the agent to copy all messages to the **Inbox** folder to allow access by IMAP.

2a. Expand **Shared Code**, click **Agents**, and click **New Agent** in the center pane:

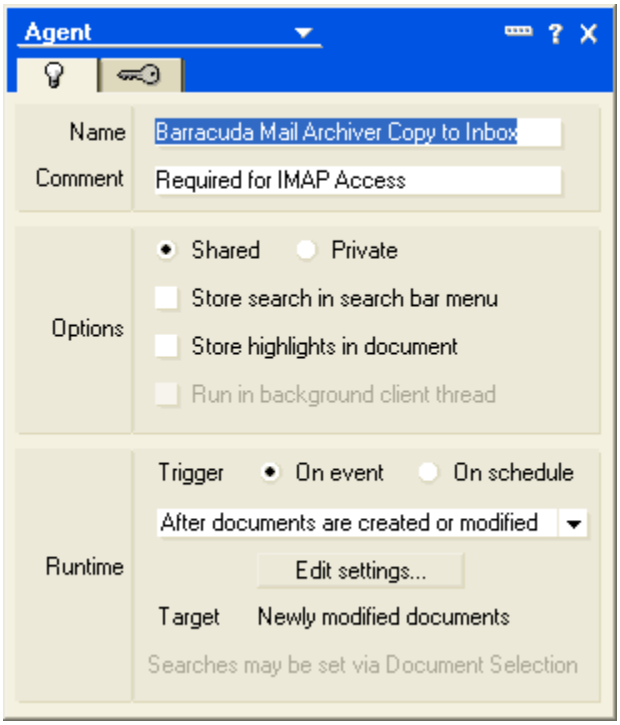


2b. The **Agent** dialog box displays:

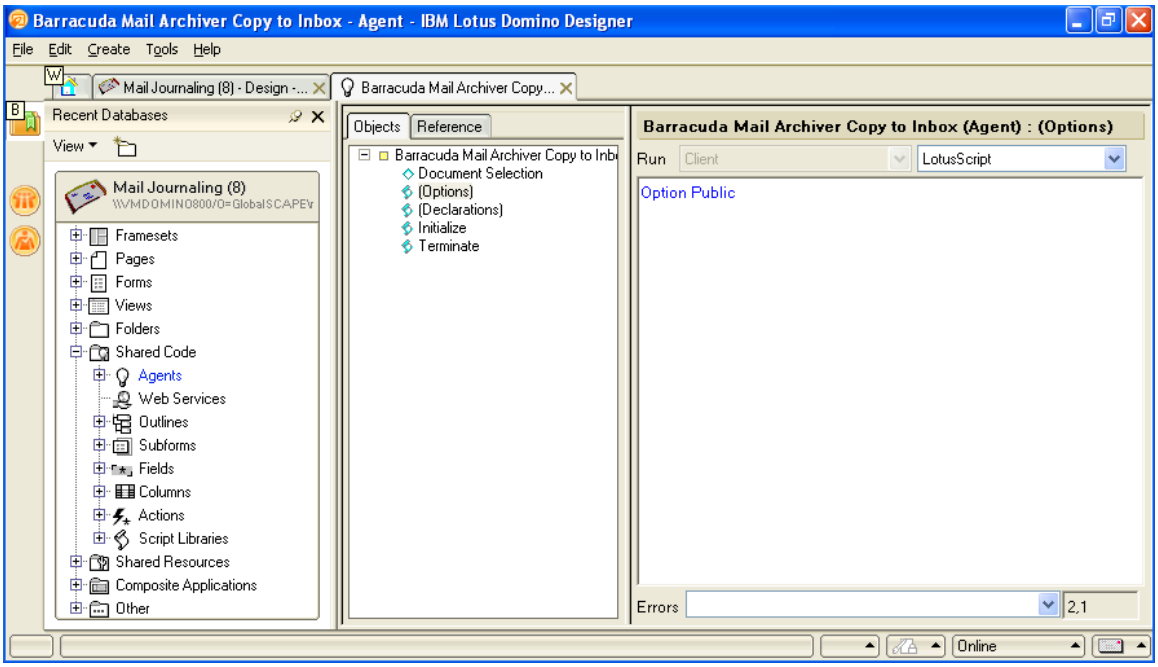


2c. In the **Name** field, type the following value: `Barracuda Mail Archiver Copy to Inbox`

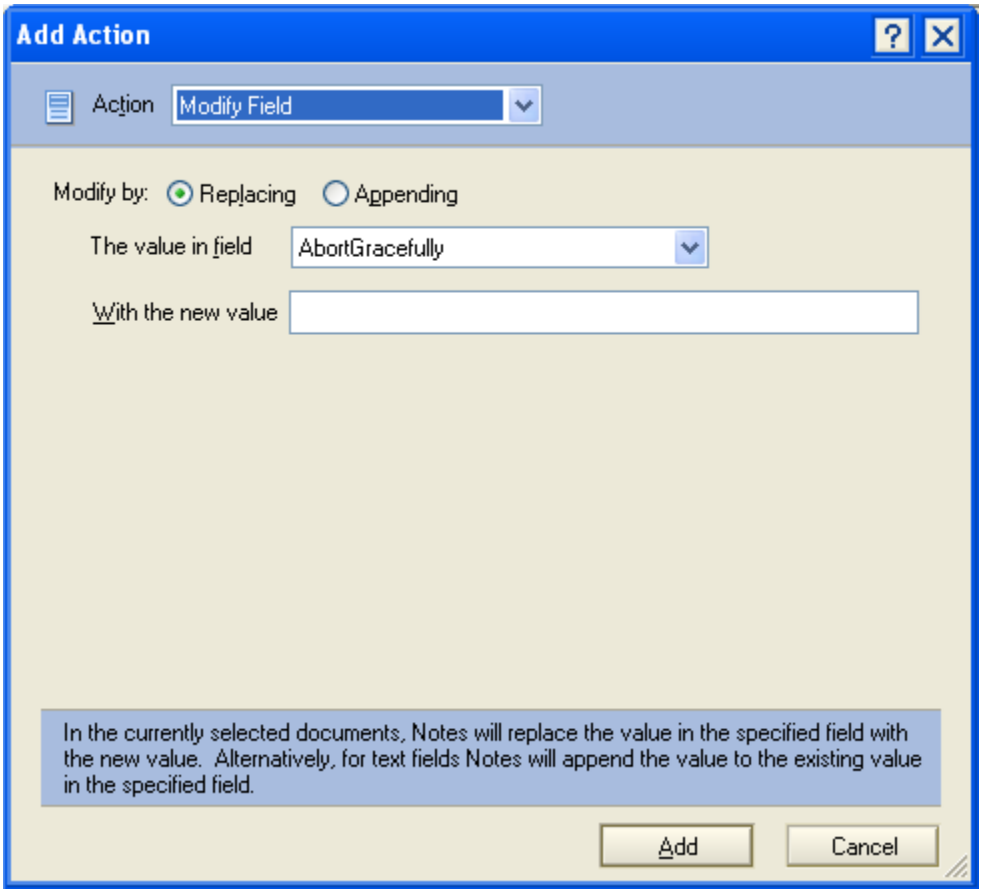
2d. In the **Comment** field, you can optionally enter a comment to describe the agent. In the **Runtime** section, set the **Trigger** to **On event**, and select **After documents are created or modified**:



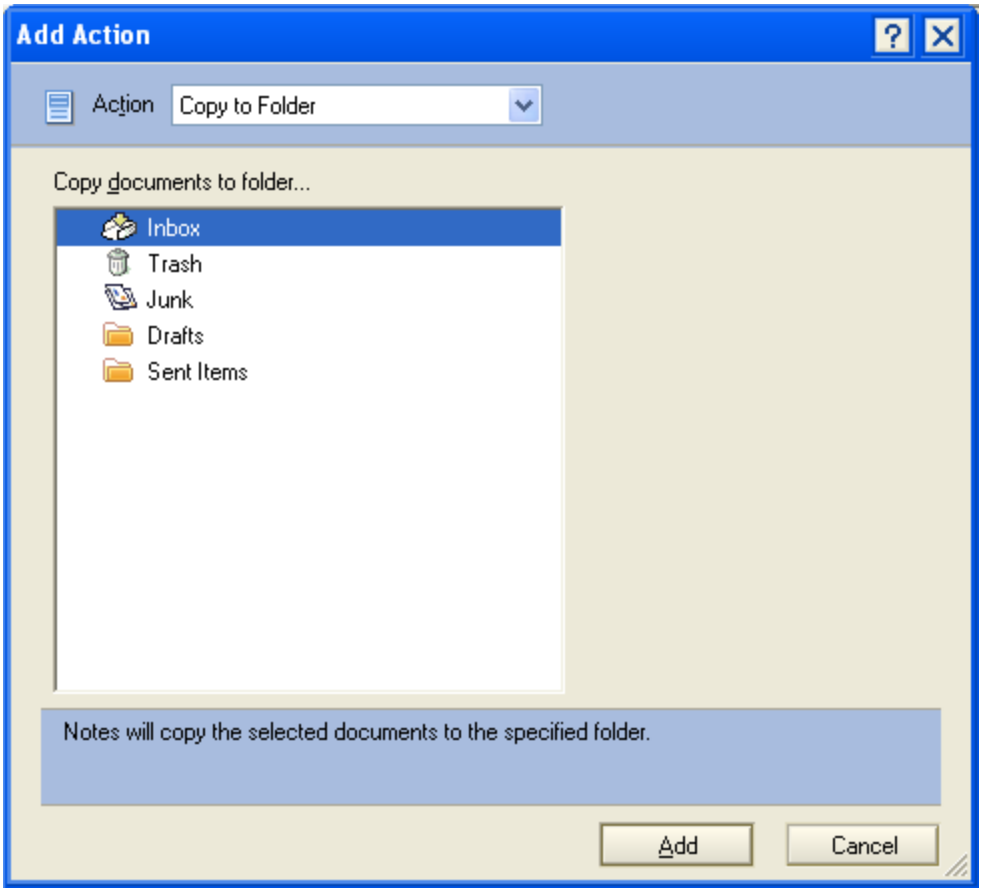
2e. Click the **Close** ( ) icon to save your changes; close the dialog box. The **Agent** displays in the right pane:



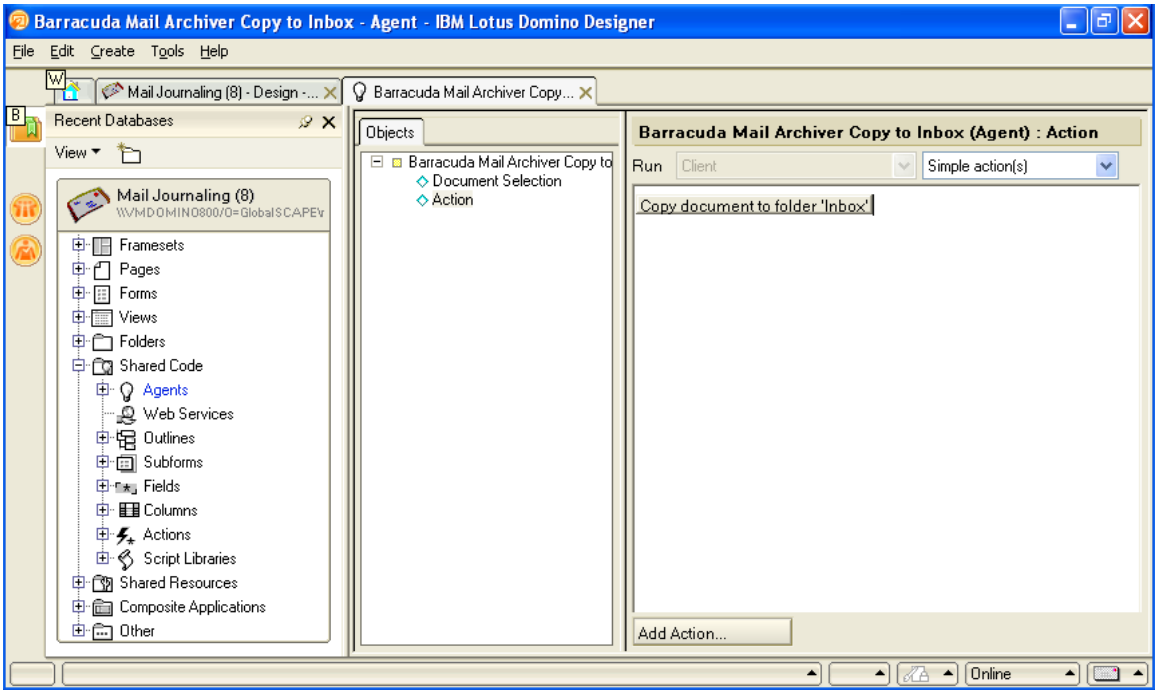
2f. In the right pane, from the drop-down menu, select **Simple Action**; a warning dialog displays. Click **Yes** to save your changes and close the warning dialog. At the bottom of the **Agent** view, click **Add Action**; the **Add Action** dialog box displays:


Add Action
Action
Modify Field
Modify by:
Replacing
Appending
The value in field
AbortGracefully
With the new value
In the currently selected documents, Notes will replace the value in the specified field with the new value. Alternatively, for text fields Notes will append the value to the existing value in the specified field.
Add
Cancel

2g. From the **Action** drop-down menu, select **Copy to Folder**; the available folders display:



2h. Click **Inbox**, and then click **Add** to save your changes and close the dialog box. The **Agent** displays the new action:



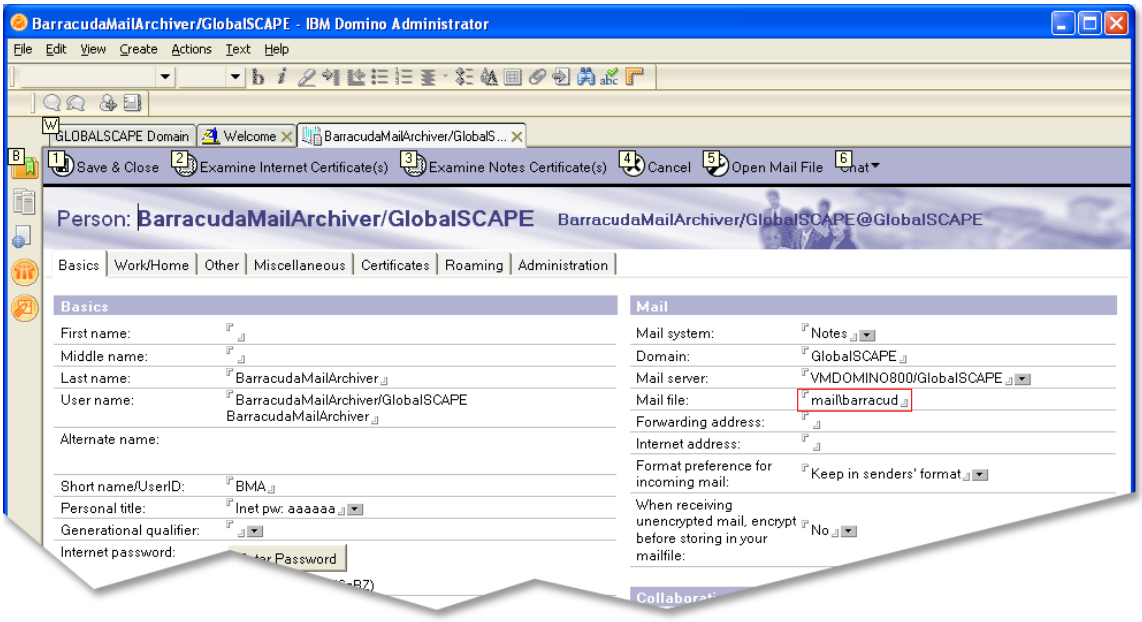
2i. Close the Agent; a warning dialog displays. Click **Yes**, and then close IBM Domino Designer.

Step 3. Update the Mail File Value

Use the following steps to change the mail file value from its existing name to **mailjrn**.

You must have an IBM Domino account with edit rights to complete the following steps.

3a. Log in to the IBM Domino Client, and open the name and address book entry for the **BarracudaMailArchiver** account. Click on the **Person** n ame in the view to access the edit mode:



3b. In the **Mail** section, note the current value of **Mail file**, then change the value to **mailjrn**:

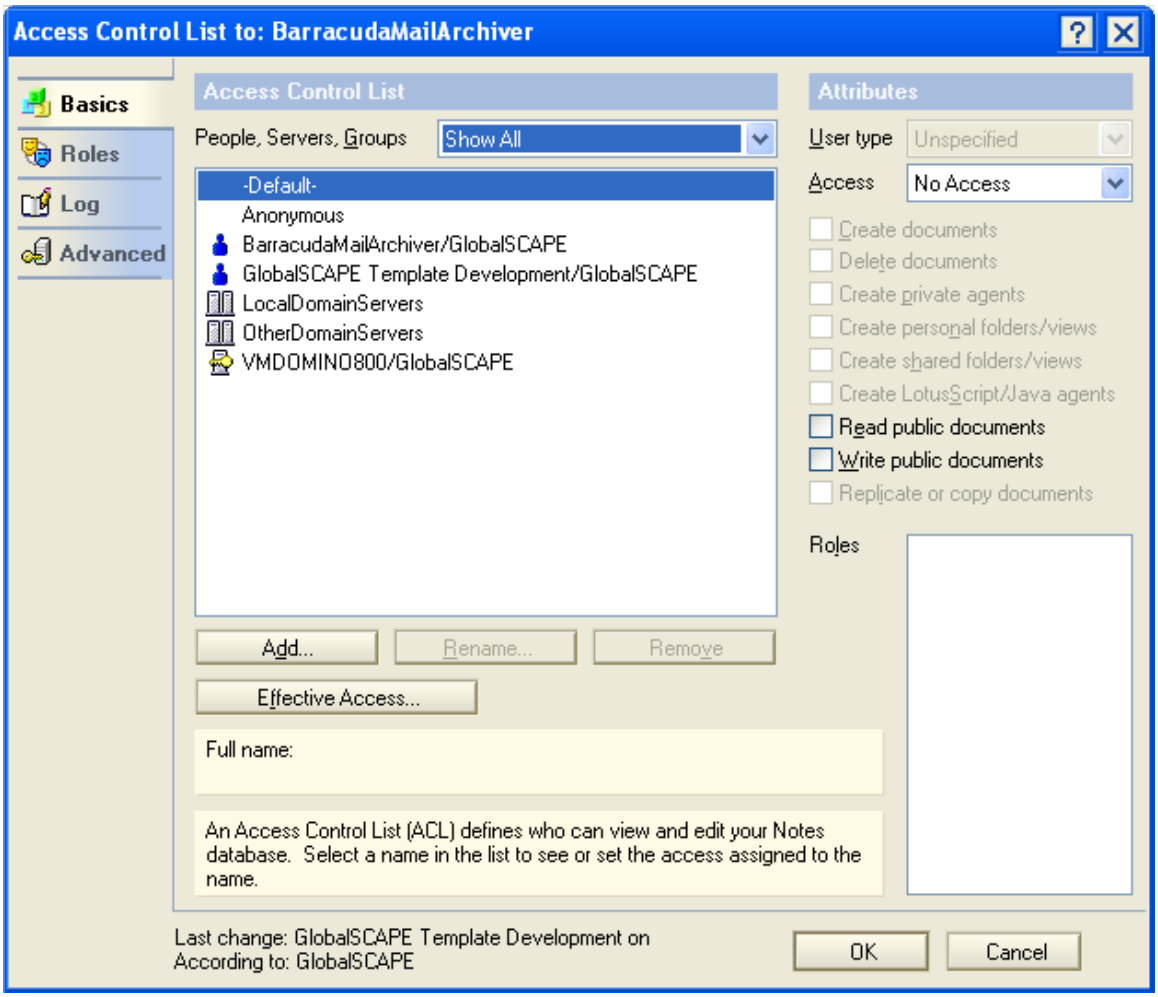
Typically the initial mail file name is preceded by a folder, e.g., **mail\databasename**, however, in this step the new value **mailjrn** is not preceded by a mail folder name.

3c. Save and close the view.

Step 4. Set Privileges

Use the following steps to verify the **Access Control List** entries for the **BarracudaMailArchiver** account on the **mailjrn.nsf** file have the same privileges as the **BarracudaMailArchiver** account on the *original* mail database.

4a. Log in to the IBM Domino Client, and open the **Files** tab. Right-click **mailjrn.nsf**, and click **Access Control - Manage**; the **Access Control List** dialog box displays:



4b. If the **BarracudaMailArchiver** account does not display, click **Add** at the bottom of the screen and add the account to the database file. Click **OK** to save changes and close the **Access Control List**.

Test Your Settings

Open an email application that supports IMAP, and verify that the **BarracudaMailArchiver** account can be read and that the Inbox contains the records from the mail archive file. The **mailjrn.nsf** file Agent runs on a schedule specified by the IBM Domino Server (the default is every 30 minutes and can be set to a minimum of 5 minute intervals), therefore messages may not be immediately available. To force the Agent to run immediately, from the Domino Console, run the following command:

```
Tell amgr run mailjpn.nsf 'Barracuda Mail Archiver Copy to Inbox'
```

MailEnable Deployment

> This article refers to the Barracuda Message Archiver firmware version 3.1 or later and the MailEnable Mail Server, Standard, Professional, or Enterprise Edition.

You can configure a global message content filter using the MailEnable Mail Transfer Agent (MTA) to forward a copy of all incoming and outgoing messages to your Barracuda Message Archiver IP address.

In this article:

- Set Up MailEnable Standard Edition
- Set up MailEnable Professional or Enterprise Edition

Additional Resource
• Barracuda Networks Knowledgebase Solution #00 003577 • How to archive the messages that are sent and received by MailEnable • MailEnable Enterprise Edition Configuration Guide • MailEnable Standard Guide - 6.0 • MailEnable Professional Guide - 6.0 • MailEnable Enterprise Guide - 6.0

Set Up MailEnable Standard Edition

MailEnable Standard Edition uses the MTA Pickup Event through the Message Snoop Utility (MESNOOP) executable to set up message archiving.

Use the following steps to enable the MTA pickup event:

1. Download **MESNOOP.ZIP** from the MailEnable website: http://www.mailenable.com/utilities/addons/MESNOOP.zip
2. Extract the files, and copy MSNOOP.EXE to the following directory:
   C:\Program Files\Mail Enable\Bin directory
3. Double-click the file, and click **Run**. The **MailEnable Message Snoop Utility** opens.
4. In the **Filtering** section, turn on **Copy All Mail**, and enter the Barracuda Message Archiver IP address in the associated field.
5. Click **OK** to save your settings. The MTA pickup event begins archiving mail to the Barracuda Message Archiver IP Address.

Set up MailEnable Professional or Enterprise Edition

Use the following steps to set up mail archival to the Barracuda Message Archiver:

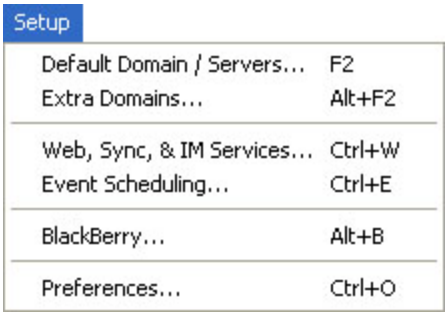
1. Log in to the MailEnable administration console, expand **Messaging** Manager, right-click **Filters**, and click **New > New filter**.
2. Turn on **Filter is enabled**, and enter the name **Archive all messages**. Save the filter.
3. In the right-pane, double-click the new filter; the **Filter Management** window displays.
4. Scroll down to and double-click the criteria **All messages - Process filter actions for all messages**; the **Properties** window displays.
5. Turn on **Enable**, and then click **OK**.
6. In the **Filter Management** window, click **Add Action**; the **Actions** list displays. Locate and double-click **Forward to address**; the **Properties** window displays.
7. In the **forwarding address** field, enter the Barracuda Message Archiver IP address in the associated field, and then click **OK**.

MDaemon Messaging Server Deployment

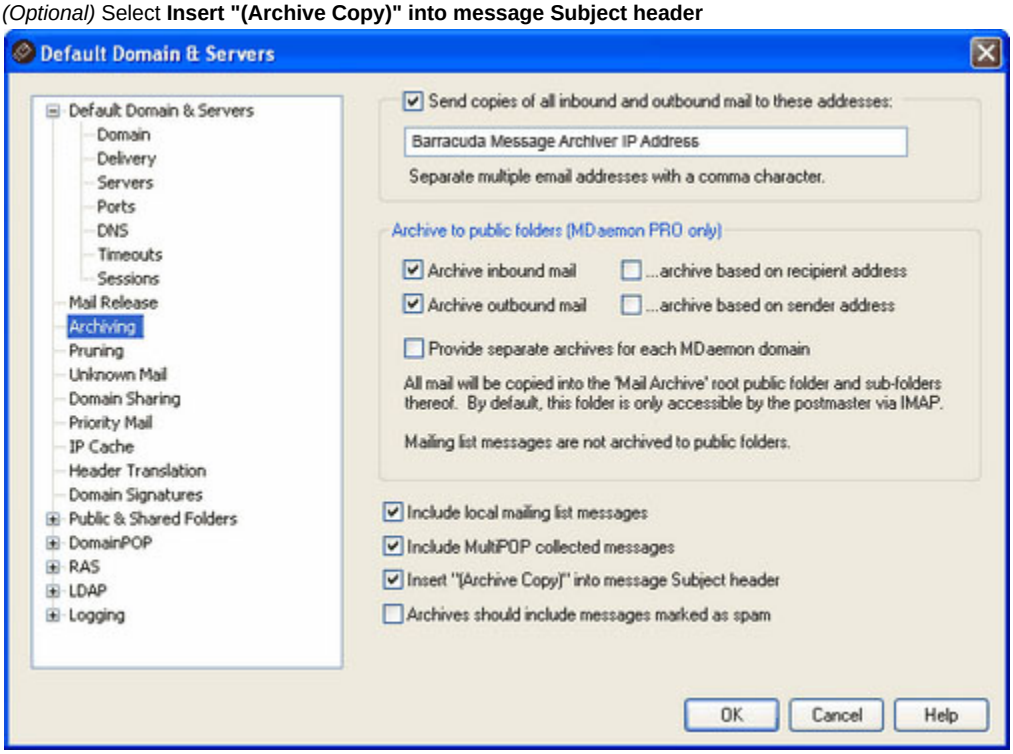
This article refers to the Barracuda Message Archiver firmware version 3.1 and higher, and the MDaemon® Messaging Server.

Use the following steps to configure an MDaemon Messaging Server to forward a copy of all incoming and outgoing messages to the Barracuda Message Archiver.

1. From the MDaemon menu bar, click the **Setup** menu, and click **Default Domain / Servers** domain:



2. In the **Default Domain & Servers** dialog box, click **Archiving**, and then:
   - Select **Send copies of all inbound and outbound mail to these addresses** and enter the email address of your Barracuda Message Archiver in the associated field, for example, **archiver@192.168.200.200<mailto:archiver@192.168.200.200>**
   - Select **Archive inbound mail**
   - Select **Archive outbound mail**
   - Select **Include local mailing list messages**
   - Select **Include MultiPOP collected messages**
   - *(Optional)* Select **Insert "(Archive Copy)" into message Subject header**



3. Click **OK** to save your changes.

Barracuda Cloud Relay Service Configuration for Office 365 Mail Service

This article applies to Barracuda Message Archiver firmware version 3.2 and higher, and Microsoft Office 365 Enterprise cloud-based mail service, live@edu.

You can configure the Barracuda Cloud Relay Service to dispatch journaled mail from the Office 365 hosted mail service to the Barracuda Message Archiver. Note that the Office 365 Management Panel web interface may differ slightly depending on the version of Office 365 you are running.

In this article:

- Step 1. Open Port 2500 on your Corporate Firewall

- Step 2. Configure Barracuda Message Archiver Forwarding
- Step 3. Create a Non-Delivery Report Recipient
- Step 4. Configure Office 365 to Send Journal Mail

Related Articles
• Office 365 IMAP/POP Deployment

Additional Resources
• Office 365: Understanding Journal Rules • Office 365: Creating a Journal Rule

Hybrid Deployment
If you are using the Barracuda Cloud Relay Service with a hybrid Microsoft Exchange Server / Office 365 deployment, where some mailboxes are located on a physical server and some mailboxes are hosted by Office 365, to properly deploy your configuration, you must journal directly to the physical Barracuda Message Archiver from your Exchange Server by designating an on-premises mailbox as the journal mailbox for your Office365 and on-premises mailboxes.

Use the following articles to set up journaling based on the version of Exchange Server running in your environment:

- How to Configure Envelope (SMTP) Journaling for Microsoft Exchange Server 2013 - Standard Journaling
- How to Configure Envelope (SMTP) Journaling for Microsoft Exchange Server 2013 - Premium Journaling
- Configuring Envelope Journaling for Microsoft Exchange Server 2007 and 2010
- Configuring an SMTP Journal Account for Microsoft Exchange 2003

Additionally, be sure to review the Microsoft technet Journaling article, specifically:
“You can't designate an Office 365 mailbox as a journaling mailbox for on-premises mailboxes. If you’re running a hybrid deployment with your mailboxes split between on-premises servers and Office 365, you can designate an on-premises mailbox as the journaling mailbox for your Office 365 and on-premises mailboxes.”

Custom Token
Before completing the steps in this deployment, contact Barracuda Networks Technical Support and request a custom token to configure Barracuda Cloud Relay Service for Office 365 Mail Service. For example, **uuid.bma.cudasvc.com**.

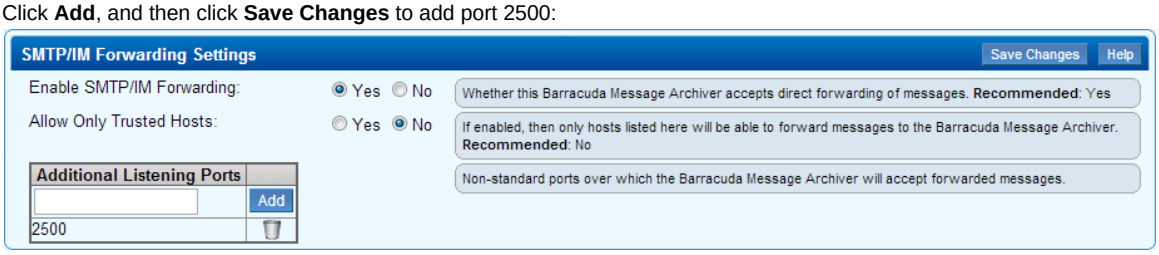
Step 1. Open Port 2500 on your Corporate Firewall

Mail journaled for Compliance purposes on Office 365 is sent to the Barracuda Cloud Relay Service on port 25. The Barracuda Cloud Relay Service then sends the mail to your Barracuda Message Archiver on port 2500. You *must* open port 2500 on your corporate firewall to allow journaled mail to be sent to the Barracuda Message Archiver.

Step 2. Configure Barracuda Message Archiver Forwarding

Use the following steps to configure the Barracuda Message Archiver to accept mail on port 2500:

1. Log in to the Barracuda Message Archiver as the administrator, and go to the **MAIL SOURCES > SMTP/IM** tab.
2. Turn on **Enable SMTP/IM Forwarding**, and type `2500` in the **Additional Listening Ports** field.
3. Click **Add**, and then click **Save Changes** to add port 2500:


SMTP/IM Forwarding Settings
Save Changes
Help
Enable SMTP/IM Forwarding:
Yes
No
Whether this Barracuda Message Archiver accepts direct forwarding of messages. Recommended: Yes
Allow Only Trusted Hosts:
Yes
No
If enabled, then only hosts listed here will be able to forward messages to the Barracuda Message Archiver. Recommended: No
Additional Listening Ports
Add
2500
Non-standard ports over which the Barracuda Message Archiver will accept forwarded messages.

Step 3. Create a Non-Delivery Report Recipient

Before creating journal rules, specify a journal recipient for non-delivery reports (NDRs) to reduce the risk of losing journal reports.

To create an NDR recipient,

1. Log in to the server as the administrator, and navigate to **Manage My Organization > Mail Control > Journaling**.
2. Next to **NDRs for undeliverable journal reports will be sent to**, click **Select address**.
3. In the **NDRs for undeliverable journal reports** window, click **Browse**.
4. Select a recipient from the address book. You can search for a recipient by typing all or part of a display name, and then clicking the **Sear ch** icon, or click on either the **Display Name** or **E-Mail Address** heading to sort the list.
5. Click **OK** once you select a recipient, and in the **NDRs for undeliverable journal reports** window, click **Save**.

Step 4. Configure Office 365 to Send Journal Mail

Before Proceeding
Verify the following:

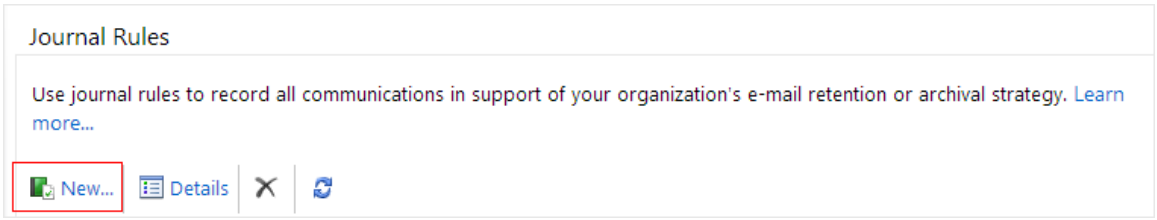
- You have the custom address and token specific to your Barracuda Message Archiver provided to you by Barracuda Networks Technical Support;
- You have your WAN IP address where you want the journal mail sent;
- The WAN IP address accepts journal email on the specified port (default port 2500); *and*
- The firewall port is NAT'd to the Barracuda Message Archiver.

Set up the “journaling mailbox” using the external address for the Barracuda Cloud Relay Service based on the custom token received from Barracuda Networks Technical Support, for example, **journaling@UUID.bma.cudasvc.com**.

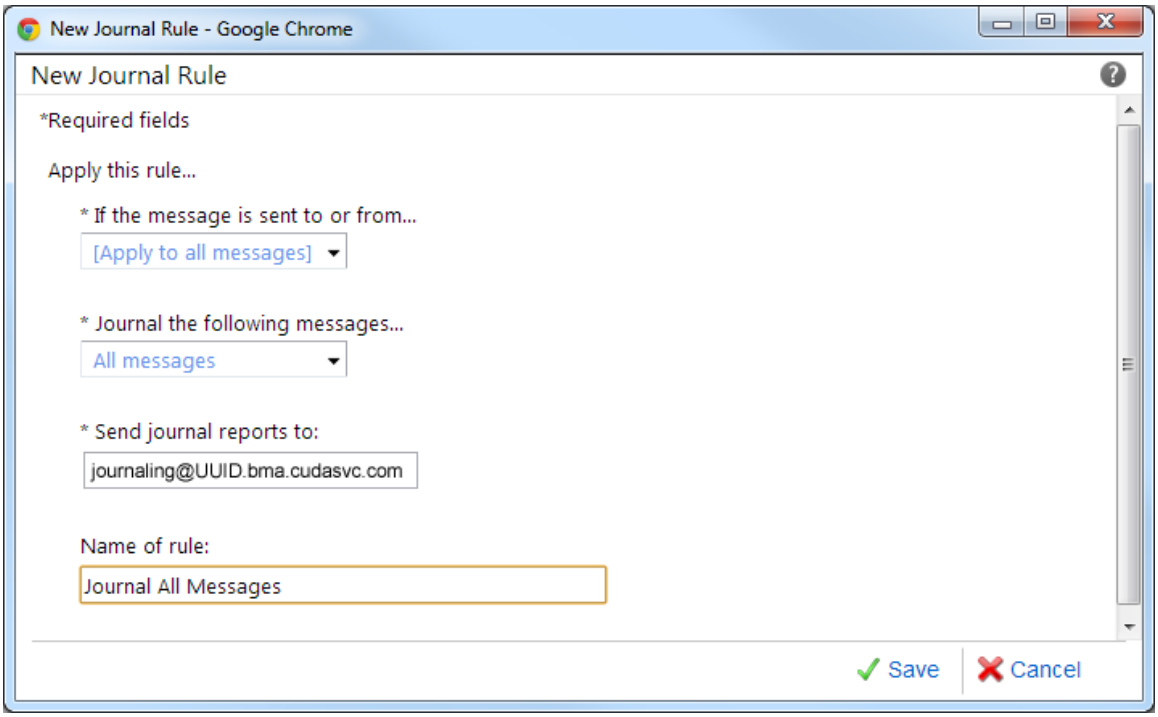
Please note: The Barracuda Cloud Relay Service cannot accept your journal mail traffic until Barracuda Support indicates that the Relay Service has been configured for your account.

Use the following steps to configure Office 365 to send journal mail to Barracuda Cloud Relay Service:

1. Log in to your Office 365 Management Panel as the Administrator.
2. Select **Manage My Organization** > **Mail Control** > **Journal Rules** > **New** :


Journal Rules
Use journal rules to record all communications in support of your organization's e-mail retention or archival strategy. Learn more...
New...
Details

3. In the **New Journal Rule** dialog box, complete the following:
   a. **If the message is sent to or from** – Select **Apply to all messages** to journal all recipients.
   b. **Journal the following messages** – Select **All messages** to journal all messages regardless of source or destination.
   c. **Send journal reports to** – Enter the email address where you want to store the journal reports generated by the journal rule. This is called the "journaling mailbox":



> Because the journaling mailbox may contain sensitive information, it is recommended that you create organization-wide policies that govern who can access the journaling mailboxes in your organization.

d. **Name of rule** – By default, the name of the journal rule is automatically generated from the journal recipients. If there are existing journal rules that contain the same journal recipients, numbers are automatically appended to the journal rule name to avoid duplicates. If you choose to override the automatically-generated name by typing in a custom name, verify the name is unique and descriptive.

4. Click **Save**.

Supplemental Service Information

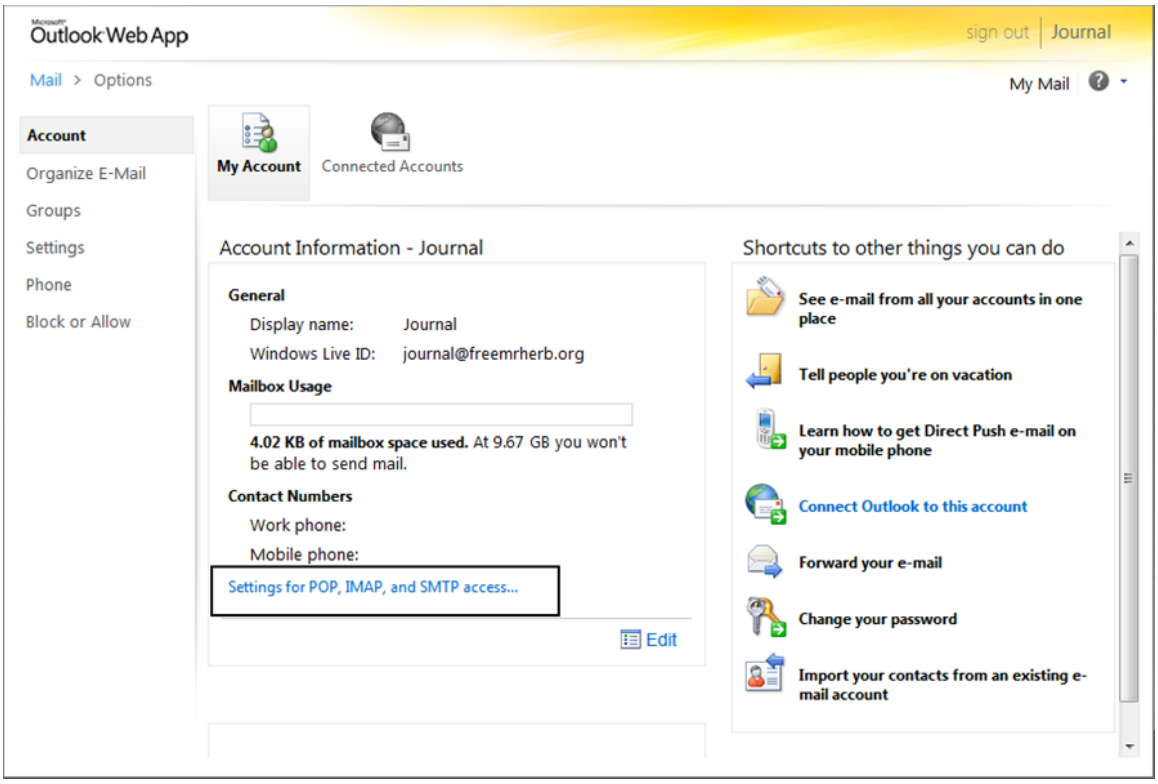
Office 365 IMAP/POP Deployment

This article refers to the Barracuda Message Archiver release 3.1 or higher, and Microsoft ® Office 365™ for Midsize Business, Enterprise, and Live.edu deployments.

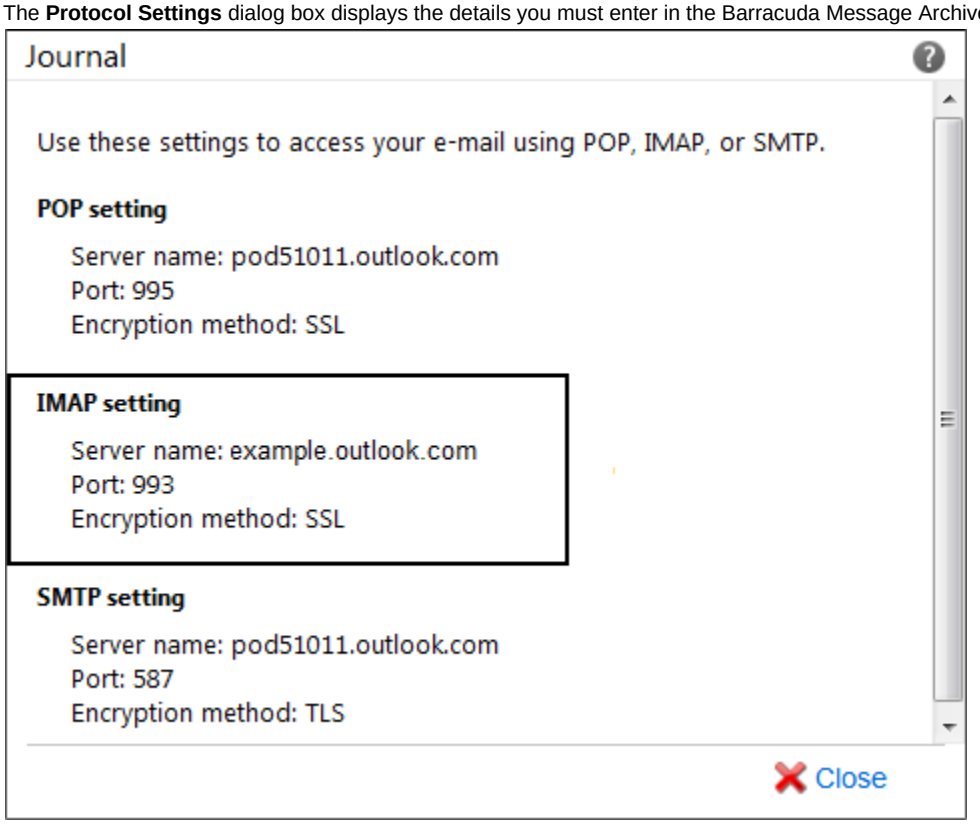
Recommended Deployment

Barracuda Networks recommends deploying your Barracuda Message Archiver with Office 365 using the Barracuda cloud relay service configuration for Office 365 mail service , alternately, you can set up IMAP/POP3 journaling as described in this article.

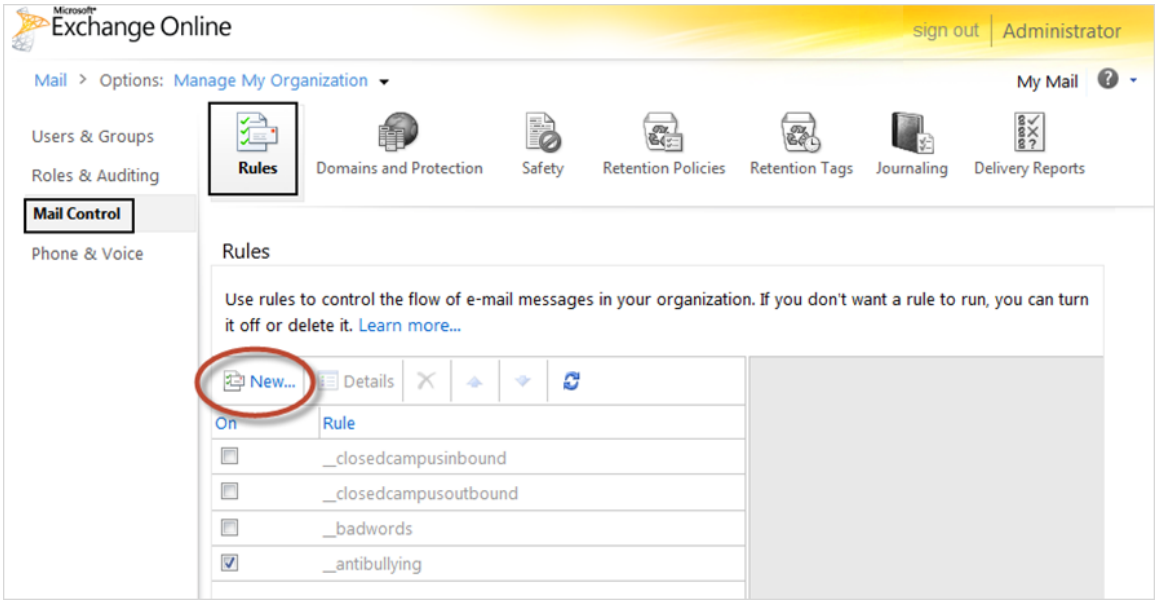
1. Log in to your Office 365 Management Panel as the Administrator.
2. Create a User Mailbox; enter the User Mailbox, for example, type `Journal` or `Archive Mailbox`.
3. Log in to Office 365 as the newly created user and specify the time zone settings.
4. From the Office 365 Management Panel, click **Settings for POP, IMAP and SMTP access**:



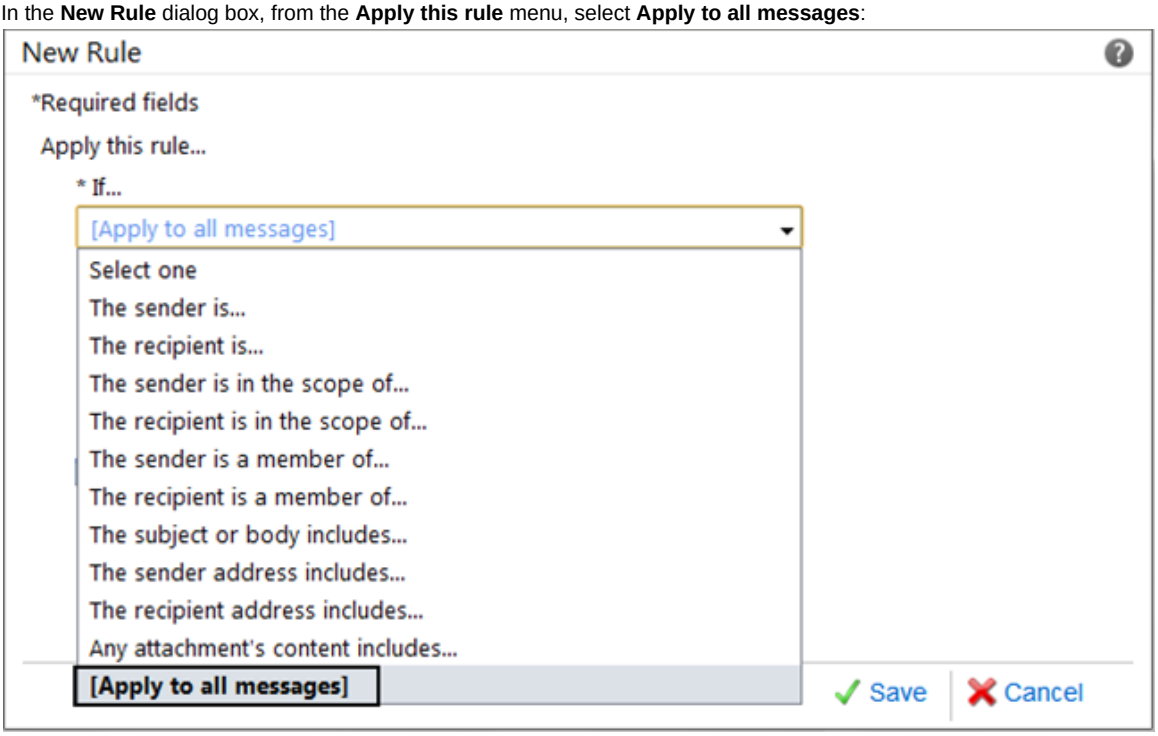
5. The **Protocol Settings** dialog box displays the details you must enter in the Barracuda Message Archiver:



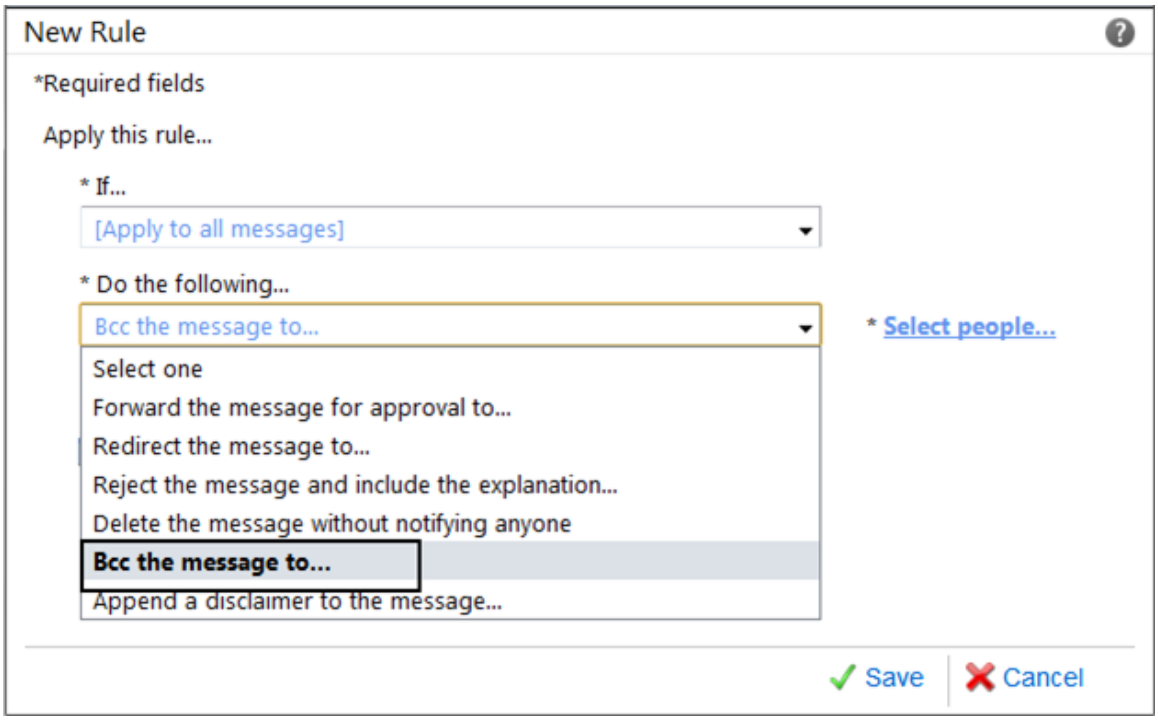
6. Open another window and log in to the Barracuda Message Archiver as the Administrator.
7. Navigate to the **MAIL SOURCES > Journal Accounts** page. In the **Journal Accounts Configuration** section, enter the details from the Office 365 **Protocol Settings** dialog box.
8. In the Office 365 Management Portal, click **Mail Control > Rules**, and then click **New**:



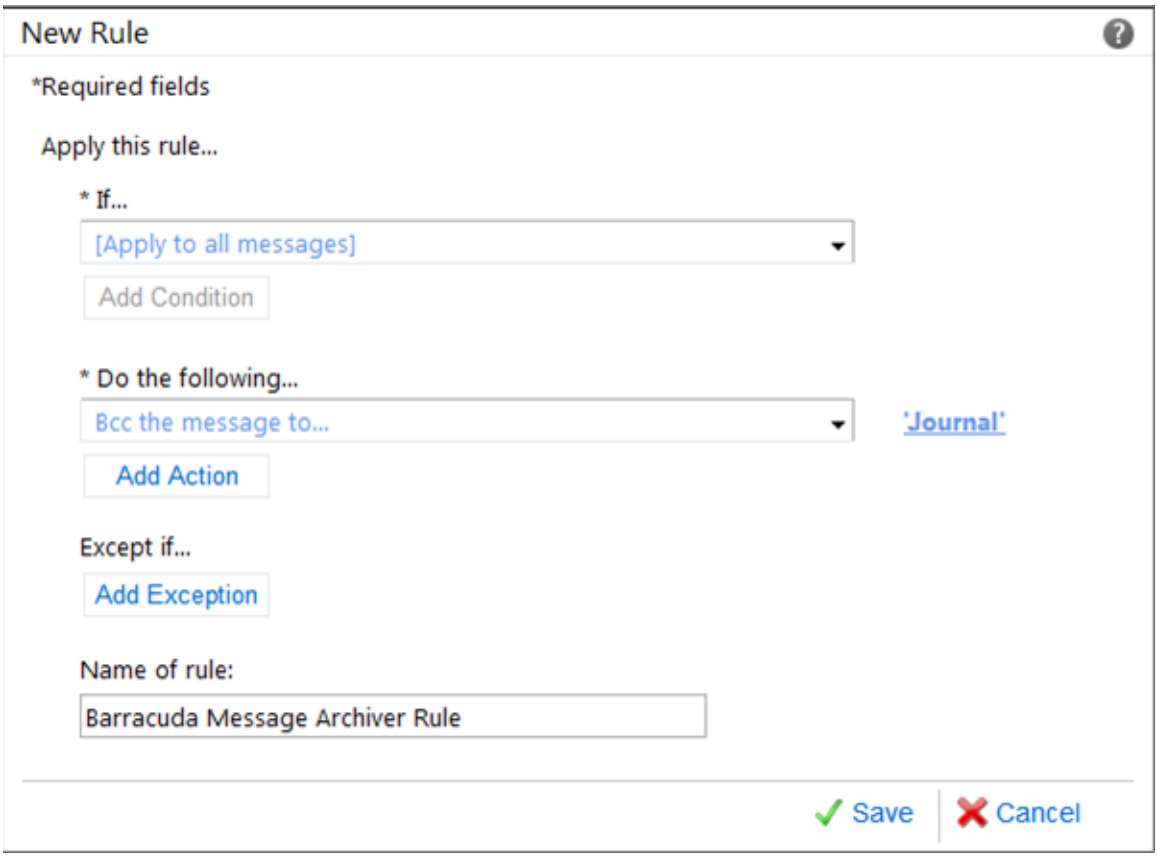
9. In the **New Rule** dialog box, from the **Apply this rule** menu, select **Apply to all messages**:



10. From the **Do the following** menu, select **Bcc the message to**:



11. In the **Select Members** dialog box, select the Journal/Archive Mailbox you created in **Step 2**, click **Add**, and then click **OK**.
12. In the dialog box, to the right of the **Do the following** menu, the selected Journal/Archive Mailbox name displays.
13. In the **Name of rule** field, enter the rule name, for example, `Barracuda Message Archiver Rule`:



14. Click **Save**. In the **Warning** dialog box, click **Yes** to save the new rule.

Unix Mail Server Deployment

This article refers to the Barracuda Message Archiver release 3.1 or later, and Unix Mail Servers including Apple Mail Server, Sendmail, Postfix, and qmail.

You can configure Sendmail, Postfix, and qmail to forward a copy of all incoming and outgoing messages as a blind-carbon-copy (bcc) to your Barracuda Message Archiver IP address. Sendmail, Postfix, and qmail support most Unix operating systems including Mac OS X.

For more information, refer to the Barracuda Networks Knowledgebase Solution How should I configure the Barracuda Message Archiver to work with Unix mail servers like Sendmail, Postfix, or qmail?

Barracuda Message Archiver and the Barracuda Spam Firewall

In this Section

- Understanding Email Encryption and Archival
- How to Set Up Email Encryption and Archival

Understanding Email Encryption and Archival

Required Product Version
This article applies to the Barracuda Message Archiver firmware version 3.2 and higher, and the Barracuda Spam Firewall firmware version 6.0 and higher.

You can encrypt and archive journaled email by partnering the Barracuda Spam Firewall and the Barracuda Message Archiver.

Related Articles

- How to Set Up Email Encryption and Archival

Barracuda Message Archiver

- Deployment Options
- Message Import, Stubbing, and Configuration Options

Barracuda Spam Firewall

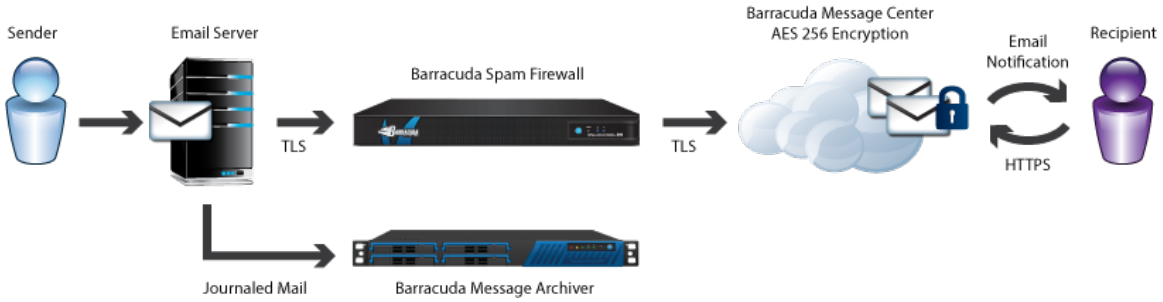
- Archiving Encrypted Email Messages
- Encryption of Outbound Mail 6.x

Organizations using a Barracuda Spam Firewall and Email Encryption Service can include a Barracuda Message Archiver to capture all Encrypted inbound and outbound messages.

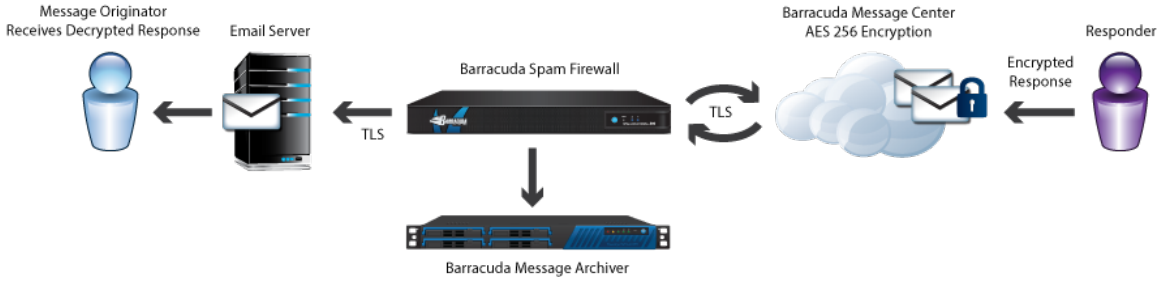
The Barracuda Spam Firewall securely encrypts email which is then sent via Transport Layer Security (TLS) to the cloud-based Message Center ensuring email is encrypted and keys are securely stored using AES 256-bit encryption. The Barracuda Message Archiver is a complete email archiving solution designed for optimizing email storage, meeting regulatory compliance and e-discovery requirements, and seamless end-user integration with Outlook and Mobile Apps to search all of your existing email.

- **Outbound mail** - When a user sends email, the email takes parallel paths: it is sent to the Barracuda Message Archiver for archival, and at the same time it is journaled on the Email Server and sent to the Barracuda Spam Firewall. The email is sent securely to the

Barracuda Message Center where it is encrypted, and a notification is sent to the intended recipient who can then log in and access the email over HTTPS:



- **Inbound mail** - When the recipient responds to the email, the response is sent back through the Message Center where it is encrypted and the Message Center notification is delivered. The Barracuda Spam Firewall then periodically contacts the Message Center for new mail sent or received for your domain, and sends the email to the Barracuda Message Archiver to ensure complete archival of Message Center correspondence:



How to Set Up Email Encryption and Archival

Required Product Version
This article applies to the Barracuda Message Archiver firmware version 3.2 and higher, and the Barracuda Spam Firewall firmware version 6.0 and higher.

You can encrypt and archive journaled email by partnering the Barracuda Spam Firewall and the Barracuda Message Archiver.

In this article:

- Requirements
- Define Encryption Policies
- Activate Encrypted Mail Archiving
- Verify Inbound and Outbound Email Archival

Related Articles

- Understanding Email Encryption and Archival

Barracuda Message Archiver

- Deployment Options
- Message Import, Stubbing, and Configuration Options

Barracuda Spam Firewall

- Archiving Encrypted Email Messages
- Encryption of Outbound Mail 6.x
- Content Analysis Outbound

Requirements

Before getting started, verify that you have the following deployed and running in your environment:

> **Important**
> Upon activating archived mail encryption, the Barracuda Spam Firewall periodically contacts the Message Center for new mail sent or received for your domain. To ensure a secure outbound connection and delivery of email to the Barracuda Message Archiver, port 4234 must be open.

- Email Server configured to utilize journaling
- Barracuda Message Archiver firmware version 3.2 or higher
- Barracuda Spam Firewall firmware version 6.0 or higher

Define Encryption Policies

> See Encryption of Outbound Mail 6.x for additional information.

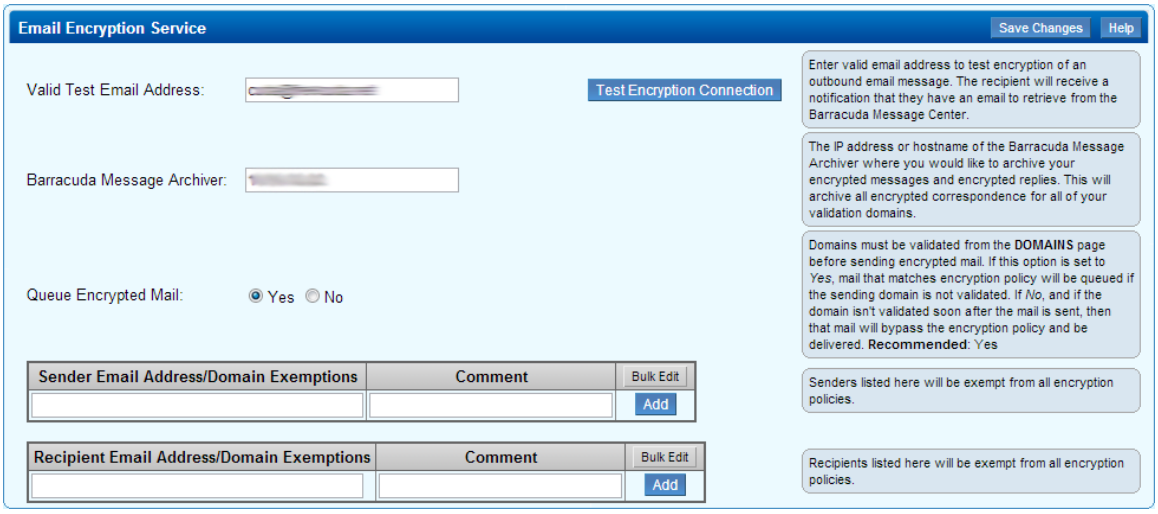
Encryption is configured at the domain level while an encryption policy is configured at the global level, for example, by sender domain or email address. Global encryption policies apply to all domains from which encrypted email messages are sent. From the **BLOCK/ACCEPT** page in the Barracuda Spam Firewall, specify the outbound encryption rules for global system-managed filtering including:

- **Content Filtering** - Specify message delivery filtering based on expressions
- **Custom Content Filters** - Filter based on subject line, message headers, message body and attachment file type
- **Attachment Filtering** - Block, quarantine, encrypt, or redirect outbound messages based on patterns or file extensions
- **Predefined DLP and HIPAA Compliance Filters** - Filter based on predefined data leakage patterns as specified on the **BLOCK/ACCEPT > Content Filters** page

Activate Encrypted Mail Archiving

Use the following steps to specify encrypted email archival on the Barracuda Message Archiver:

1. Log in to the Barracuda Spam Firewall as the administrator, and go to the **BASIC > Administration** page.
2. In the **Email Encryption Service** section, enter an email address in the **Valid Test Email Address** field to test encryption, and enter the Barracuda Message Archiver the IP address in the associated field:


Email Encryption Service
Save Changes
Help
Valid Test Email Address:
Test Encryption Connection
Enter valid email address to test encryption of an outbound email message. The recipient will receive a notification that they have an email to retrieve from the Barracuda Message Center.
Barracuda Message Archiver:
The IP address or hostname of the Barracuda Message Archiver where you would like to archive your encrypted messages and encrypted replies. This will archive all encrypted correspondence for all of your validation domains.
Queue Encrypted Mail:
Yes
No
Domains must be validated from the DOMAINS page before sending encrypted mail. If this option is set to Yes, mail that matches encryption policy will be queued if the sending domain is not validated. If No, and if the domain isn't validated soon after the mail is sent, then that mail will bypass the encryption policy and be delivered. Recommended: Yes
Sender Email Address/Domain Exemptions
Comment
Bulk Edit
Add
Senders listed here will be exempt from all encryption policies.
Recipient Email Address/Domain Exemptions
Comment
Bulk Edit
Add
Recipients listed here will be exempt from all encryption policies.

3. Specify any additional **Email Encryption Service** settings, and then click **Save Changes**.
4. Log in to the Barracuda Message Archiver as the administrator, and go to **MAIL SOURCES > SMTP/IM** page.
5. In the **Enable SMTP/IM Forwarding** section, set **Enable SMTP/IM Forwarding** to **Yes**.
6. In the **Trusted SMTP Servers** section, add the Barracuda Spam Firewall IP address, click **Add**, and then click **Save Changes**.

Verify Inbound and Outbound Email Archival

1. Log in to the Barracuda Spam Firewall as the administrator, and go to the **BASIC > Administration** page.
2. In the **Email Encryption Service** section, click **Test Encryption Connection**. The recipient will receive a notification once the test email

is available in the Barracuda Message Center.

Getting Started

Recommended Steps

- Step 1: How to Install the Barracuda Message Archiver
- Step 2: How to Configure the Barracuda Message Archiver
- Step 3: How to Configure the Web Interface
- Step 4: How to Configure Administrative Settings
- Step 5: Understanding Message Archiving Concepts

Alternatively, you can download the Barracuda Message Archiver Quick Start Guide.

Step 1: How to Install the Barracuda Message Archiver

This article refers to the Barracuda Message Archiver firmware version 3.1 and higher.

Deployment Options
Before installation, determine the best type of deployment for your Barracuda Message Archiver; refer to the Deployment section for a list of options.

Verify Equipment

Verify you have the necessary equipment:

- Barracuda Message Archiver (check that you have received the correct model)
- AC power cord
- Ethernet cables
- VGA monitor (recommended)
- USB /PS2 keyboard (recommended)

Connect to Network

1. Fasten the Barracuda Message Archiver to a standard 19-inch rack or other stable location.

   Do not block the cooling vents located on the front and rear of the unit.
2. Connect a CAT5 or a CAT6 Ethernet cable from your network switch to the Ethernet port on the back of the Barracuda Message Archiver.
3. Connect the following to your Barracuda Message Archiver:
   - Power cord
   - VGA monitor
   - USB/PS2 keyboard
4. After you connect the AC power cord, the Barracuda Message Archiver may power on for a few seconds and then power off; this behavior is normal.
5. Press the Power button located on the front of the unit.
   The administrative console login prompt displays on the monitor, and the power light on the front of the Barracuda Message Archiver turns on.

Continue with Step 2: How to Configure the Barracuda Message Archiver.

Step 2: How to Configure the Barracuda Message Archiver

This article refers to the Barracuda Message Archiver release 3.1 or higher.

Before configuring the IP address and network settings, complete Step 1: How to Install a Barracuda Message Archiver.

Configure the IP Address and Network Settings

The Barracuda Message Archiver is assigned a default IP address of 192.168.200.200.

To set a new IP address from the administrative console:

1. Connect your keyboard and monitor directly to the Barracuda Message Archiver.
2. At the `barracuda login` prompt, enter **admin** for the login and **admin** for the password. The **User Confirmation Requested** window displays the current IP configuration of the Barracuda Message Archiver.
3. Using your **Tab** key, select **Change** and press **Enter** to change the IP configuration.
4. Enter the new IP address, netmask, and default gateway for your Barracuda Message Archiver.
5. Enter the IP address of your primary and secondary DNS servers.
6. Click **Save** to enter your changes, and then click **Exit** to apply the new IP address and network settings to your Barracuda Message Archiver.

Configure Your Corporate Firewall

If your Barracuda Message Archiver is located behind a corporate firewall, refer to the following table for the ports that must be opened on your corporate firewall to allow communication between the Barracuda Message Archiver, your email server, and the Internet:

Port	Direction	Protocol	Description
22	Out	TCP	Remote diagnostics and technical support services
25 (optional) [(1)]	In/Out	TCP	Email notifications and alerts
53	Out	TCP/UDP	Domain Name Server (DNS)
80	Out	TCP	Firmware and Energize updates (unless configured to use a proxy)
123	Out	UDP	Network Time Protocol (NTP)
443 (optional)	In	TCP	For remote access over SSL (https) to the Barracuda Message Archiver; see Enabling SSL for Administrators and Users.
8000 (default)	In	TCP	Web and add-in access to the Barracuda Message Archiver [(2)]

Notes:
[(1)] Port 25 is the default port used for SMTP traffic. Some organizations choose to have email notifications and alerts from the Barracuda Message Archiver sent to an external email address directly or by using an external Smart Host without relaying through the corporate mail server. In these situations, the corporate firewall must be modified to allow outgoing emails from the Barracuda Message Archiver over the SMTP port.

[(2)] Whenever your Barracuda Message Archiver IP address is changed on the **BASIC > IP Configuration** page, you are disconnected from the administration interface. You must log in again using the new IP address.

Important
In general, the Barracuda Message Archiver should not accept incoming SMTP requests from systems outside your organization's network. However, if your email server is located in a DMZ, it may be necessary to configure your corporate firewall to allow incoming traffic over the designated SMTP port from your email server to the Barracuda Message Archiver.

The port specified as the Web Interface Port must be configured on your corporate firewall to allow traffic to the Barracuda Message Archiver if you want to allow remote users to use either the web interface or the Barracuda Message Archiver Outlook Add-in.

Continue with Step 3: How to Configure the Web Interface.

Step 3: How to Configure the Web Interface

This article refers to the Barracuda Message Archiver release 3.1 or higher.

Before configuring the web interface, complete Step 2: How to Configure the Barracuda Message Archiver.

In this article:

- Configure the Barracuda Message Archiver from the Web Interface
- Activate Subscriptions
- Update the Barracuda Message Archiver Firmware
- Update Definitions

Configure the Barracuda Message Archiver from the Web Interface

Verify the system accessing the web interface is connected to the same network as the Barracuda Message Archiver, and that the appropriate routing is in place to allow connection to the IP address of the Barracuda Message Archiver via a web browser.

Secure Access
To ensure the highest security, use HTTPS to configure your Barracuda Message Archiver web interface. In addition, Barracuda Networks recommends requiring HTTPS to connect to the Barracuda Message Archiver. To configure this setting, go to the **ADVANCED > Secure Administration** page in the Barracuda Message Archiver web interface.

To configure administrative settings on the Barracuda Message Archiver:

1. From a web browser, enter `http://` followed by the IP address of the Barracuda Message Archiver, followed by the default Web Interface HTTP Port (:8000).
For example, `http://192.168.200.200:8000`

2. Log in to the administration interface using **admin** for both the username and password.

3. Go to the **BASIC > IP Configuration** page and perform the following steps:

3a. In the **TCP/IP Configuration** section, verify the IP address, netmask, default gateway for your Barracuda Message Archiver.

3b. Verify the primary and secondary DNS servers for your Barracuda Message Archiver.

3c. Enter the default hostname and default domain name of the Barracuda Message Archiver.

3d. To allow external access to the Barracuda Message Archiver, you must enter an External System Name and Port that is accessible (resolvable) from outside of your organization's internal network. These may differ from the values in **Step 3c** above, since the Default Host Name may resolve to an internal IP address that is unreachable by remote users. The values specified here must be externally resolvable, and are used for stubbing operations, as well as by the Barracuda Message Archiver Outlook Add-in, to communicate with the Barracuda Message Archiver.

4. Click **Save Changes**.

Whenever your Barracuda Message Archiver IP address is changed on the **BASIC > IP Configuration** page, you are disconnected from the administration interface; log in again using the new IP address.

5. Go to the **BASIC > Administration** page and perform the following steps:

5a. Assign a new administration password to the Barracuda Message Archiver.

This is an optional step that is *highly recommended* for your own security and protection.

5b. Make sure the local time zone is set correctly.

Time on the Barracuda Message Archiver is automatically updated via NTP, and requires that port 123 is opened for outbound User Datagram Protocol (UDP) traffic on your firewall (if the Barracuda Message Archiver is located behind one).

It is important that the time zone is set correctly as this information is used to determine the integrity of the message archive, and in all logs and reports.

5c. You can change the port number used to access the Barracuda Message Archiver administration interface. The default port is 8000.

5d. Enter the amount of time for the session expiration length (in minutes) of your web administration interface session.

5e. At expiration, you are required to log back in to the administration interface.

5f. Enter the email addresses for your Administrator to receive system alerts and notifications, and other urgent communications from Barracuda Networks.

5g. *(Optional)* Specify your local SMTP server in the **Outbound SMTP Host/Smart Host** field.

5h. *(Optional)* Specify whether to require secondary authorization for certain actions.

6. Click **Save Changes**.

Activate Subscriptions

After installation, your Energize Updates and other optional subscriptions must be activated to fully enable the Barracuda Message Archiver and to continue receiving the latest updates to all virus, policy, and document definitions from Barracuda Central. The Energize Updates service is responsible for downloading these updates to your Barracuda Message Archiver.

To activate your subscription status:

1. At the top of every page, you may see the following warning:

Error: Activation has not been completed. Please activate your Barracuda Message Archiver to enable functionality. (Click here to activate)

2. Click on the designated link to go to the **Product Activation** page in a new browser window.

3. On the **Product Activation** page, fill in the required fields and click **Activate**. A confirmation page opens and displays the terms of your subscription.

- If your Barracuda Message Archiver cannot communicate directly to Barracuda Central servers, an Activation Code displays; enter this code in the **Activation Code** area using the steps described below in **step 4**.

4. Return to the Barracuda Message Archiver administration interface and navigate to the **BASIC > Status** page. In the **Subscription Status** section, verify that the word **Current** appears next to **Energize Updates** , **Instant Replacement Service** (if purchased), and **Premium Support** (if purchased). If you received an Activation Code, enter the code in the **Activation Code** area, and click **Save** to activate your Barracuda Message Archiver.

5. There may be a delay of a few minutes for the display to reflect your updated subscription status. If the status continues to display as **Unactiva ted**, click **Refresh** in the **Subscription Status** section.

If your subscription status does not change to **Current** within an hour, or if you have trouble filling out the **Product Activation** page, contact your Barracuda Networks sales representative.

Update the Barracuda Message Archiver Firmware

Use the following steps to update the firmware.

1. Go to the **ADVANCED > Firmware Update** page, and verify the installed version matches the **Latest General Release**. The **Download Now** button next to **Latest General Release** is disabled if the Barracuda Message Archiver is up-to-date with the latest firmware.

2.** If the installed version does not match **Latest General Release : read the release notes to learn about the latest features and fixes provided in the new firmware version, and click **Download Now** to begin the download. Updating the firmware may take several minutes; do not turn off the unit during this process. Click the **Refresh** button next to the firmware download progress to view the download status. A **Firmware downloaded** message displays once the download is complete, and the **Refresh** button is replaced by **Apply Now.**

3. Click **Apply Now** when the download is complete.

4. Click **OK** when prompted to reboot the Barracuda Message Archiver. A Status page displays the progress of the reboot. Once the reboot is

complete, the login page appears.

Update Definitions

To apply the newest definitions provided by Energize Updates:

1. Go to the **ADVANCED > Energize Updates** page.

2. Set **Automatic Updates** to **On**. The recommended setting is **On** for all available definitions.

3. Verify the current version is the same as the latest general release. If the rules are not up-to-date, continue to the next step, otherwise definition update is complete.

4. Click **Update** to download and install the latest available definitions to the Barracuda Message Archiver.

Continue with Step 4: How to Configure Administrative Settings.

Step 4: How to Configure Administrative Settings

This article refers to the Barracuda Message Archiver release 3.1 or higher.

Before configuring administrative settings, complete Step 3: How to Configure the Web Interface.

In this article:

- Set Administration Interface Access
- Set the System Time Zone
- Customize the Web Interface Appearance
- Enable SSL for Administrators and Users

Related Articles

- Understanding SMTP Forwarding and Trusted Servers

Set Administration Interface Access

The **BASIC > Administration** page is where you perform the following tasks related to Barracuda Message Archiver web access:

- Change the password of the administration account **admin**.
- Change the port used to access the Barracuda Message Archiver over the web (default is port 8000).
- Change the length of time after which idle users are to be logged out of the web interface (the default value is 20 minutes).
- Specify the IP addresses or netmask of the systems that can access the web administration interface. Attempts to log in as admin from other systems are denied.
- Specify the IP addresses or netmask of the systems that can communicate with the Barracuda Message Archiver via SNMP (available on Barracuda Message Archiver model 450 and higher).

Set the System Time Zone

You can set the time zone of your Barracuda Message Archiver from the **BASIC > Administration** page. The current time on the system is automatically updated via Network Time Protocol (NTP). When the Barracuda Message Archiver resides behind a firewall, NTP requires port 123 to be opened for outbound UDP traffic.

- It is important that the time zone is set correctly because this information is used in all logs and reports.
- The Barracuda Message Archiver automatically reboots when you change the time zone.

Customize the Web Interface Appearance

The **ADVANCED > Appearance** page allows you to customize the default images used on the web interface. This tab is available only on the Barracuda Message Archiver 650 and above.

Enable SSL for Administrators and Users

Use the **ADVANCED > Secure Administration** page to modify various settings related to SSL (https) access to the Barracuda Message Archiver web interface.

SSL not only ensures that your passwords are encrypted, but also ensures that all data transmitted to, and received from, the administration interface is encrypted. The Barracuda Message Archiver supports SSL access without any additional configuration. However, some sites may enforce the use of a secured connection to access the web interface, or prefer to use their own trusted certificates.

The SSL configuration referred to here is related only to the web-based administrative interface; it is unnecessary to explicitly configure SSL for traffic between the Barracuda Message Archiver and your email servers.

To enforce SSL-only access:

1. Go to the **ADVANCED > Secure Administration** page, and set the following options:
   - **HTTPS/SSL Access Only** – Specify whether users are required to use HTTPS to access the web interface.
   - **Use HTTPS links in Emails –** Specify whether notices and emails from the Barracuda Message Archiver use HTTP or HTTPS links.
   - **Web Interface HTTPS/SSL** – Enter the appropriate port number; the default value is 443.
2. Click **Save Changes** to save and activate your settings.

To change the certificate that is used, you must first create and upload the new certificate before changing the **Certificate Type** in the **SSL Certificate Configuration** section. The Barracuda Message Archiver supports the following certificate types:

- **Default (Barracuda Networks)** certificates are signed by Barracuda Networks. On some browsers, these may generate some benign warnings which can be safely ignored. No additional configuration is required to use these certificates which are provided free of charge as the default certificate type.

  > During a configuration backup, the certificate type is reset to **Default** if the original certificate cannot be located. Go to the **ADVANCED > Secure Administration** page, and in the **SSL Certificate Configuration** section, reselect the certificate from the **Certificate Type** drop-down menu to reactivate your certificate once the restore is complete.

- **Private (Self-signed)** certificates provide strong encryption without the cost of purchasing a certificate from a trusted Certificate Authority (CA). These certificates are created by providing the information requested in the **Certificate Generation** section of the **ADVANCED > Secure Administration** page. Additionally, you can download the Private Root Certificate and import it into your browser to allow verification of certificate authenticity and to prevent warnings from displaying when accessing the web interface.
- **Trusted (Signed by a trusted CA)** certificates are issued by trusted CAs, and must be purchased separately with a Certificate Signing Request (CSR). This can be downloaded after providing the information requested in the **Certificate Generation** section of the **ADVANCED > Secure Administration** page. Once you receive the third-party certificate from the CA, you must upload it to the Barracuda Message Archiver from the **Trusted Certificate** section of that same page. The certificate is in effect once the upload is completed.

Continue with Step 5: Understanding Message Archiving Concepts.

Configuration Management and Access

This article refers to the Barracuda Message Archiver release 3.1 or higher, except where noted.

In this article:

- Password Change
- Time
- Default Barracuda Locale
- Administrator IP/Range
- Web Interface Settings
- SNMP Manager
- Email Notifications
- SMB Export Options
- Search Page Settings
- Secondary Authorization
- System Reload/Shutdown

Related Articles

- Storage Backup
- Search Options & Configuration

On the **BASIC > Administration** page, you configure additional usage settings, management, and access to the Barracuda Message Archiver including many of the default display settings.

Password Change

In the **Password Change** section you change the system password for the admin account. Enter the Old and New Passwords, and re-enter the new password to change the password used to access the web interface for the Barracuda Message Archiver. Click **Save Password** to save your changes.

Time

The current time is automatically updated on the Barracuda Message Archiver via Network Time Protocol (NTP). When the Barracuda Message Archiver resides behind a firewall, NTP requires port 123 to be opened for outbound and inbound UDP traffic.

> It is important that the time zone be correctly set on the Barracuda Message Archiver. This current time determines the delivery times for messages and appears in certain mail reading programs. The system reboots when the time zone is changed.

Default Barracuda Locale

Select the default language and set the default encoding for handling unknown character sets.

> All email notifications from the Barracuda will be in UTF8 encoding.

Administrator IP/Range

Enter the IP addresses/networks allowed to access the administrative web interface for the Barracuda Message Archiver in the **Administrator IP/Range** section. Enter a Netmask of `255.255.255.255` to specify an individual IP (instead of an entire network).

> If no IP addresses or networks are specified here, then administrative access will be possible from all systems.

Web Interface Settings

Enter the Barracuda Message Archiver web interface settings in this section:

- **Web Interface HTTP Port** – The port over which the web interface is accessed. Changing this value requires changing the port used to access the interface in the browser. When machines are clustered, this value is not synchronized between machines so all machines *mu st* be configured with the same port number.
- **Session Expiration Length** – The amount of time (in minutes) allowed with no activity in the web interface, before the user session expires and the user is required to log in again.

SNMP Manager

(Available on models 450 and higher)
Enter the settings for SNMP access between the Barracuda Message Archiver and an SNMP monitor or some other program for querying system information in this section:

- **Enable SNMP Agent** – Allows the Barracuda Message Archiver to accept and respond to SNMP queries.
- **SNMP Version** – Version of SNMP to be used by the Barracuda Message Archiver. **v3** is the recommended setting as it is more secure.
  - **v2c** – Allows open access to your SNMP traffic.
    - **SNMP Community String** – The community string, or password, used to define (authenticate) SNMP access. The default community string used by the Barracuda Message Archiver to communicate SNMP information is **public**.
  - **v3** – Encrypts SNMP traffic and limits access to only password-authenticated users. *Recommended.*
    - **User** – A name to be used for authenticating SNMP v3 queries. An actual user account with this name need not exist on the Barracuda Message Archiver.
    - **Password** – The password to be used for the above account. Must be at least 12 characters long.
    - **Authentication Method** – The authentication method supported by your SNMP monitor. **SHA** is the more secure method.
    - **Encryption Method** – The encryption method supported by your SNMP monitor. **AES** is the more secure method.
- **Allowed SNMP IP/Range** – The only IP address(es) allowed to connect to the Barracuda Message Archiver via SNMP.

> If no IP addresses or networks are specified here, then SNMP access is possible from any system.

From the **BASIC > Administration** page, click on **Help** for more details on SNMP monitoring.

Email Notifications

> Separate multiple addresses in a list with commas.

You can specify email addresses to receive notifications for the following:

- **Mobile Apps Support Email Address** (Available in release 3.5 and higher only) – Recipient email address within your organization where support queries from mobile application users are sent.
- **System Contact Email Address** – Notification about new firmware releases, security bulletins, and customer service issues.

  > The contents of this field are transmitted to Barracuda Central.
- **System Email Reply Address** – The "From" address for all correspondence sent out by the Barracuda Message Archiver to users.
- **Send Welcome Emails** – When turned on, a welcome email containing the account information is sent to new users.
- **System Alerts Email Address(es)** – Recipients of all automated alerts sent directly by the Barracuda Message Archiver.
- **Report Exchange Action Errors** (Available in release 3.5 and higher only) – Sends an email alert when a Microsoft Exchange action experiences an error
- **Report Journal Account Errors** – Email alert when a journal account experiences an error.

  > Any such errors immediately displays to the admin user on all pages of the web interface, irrespective of this setting. Alerts are sent out after the specified time interval (**30 minutes**, **1 hour**, or **4 hours**) has passed, just in case the outage was temporary and corrected itself. To keep the number of possibly premature interruption notices to a minimum while still receiving word of urgent problems as soon as possible, start with the shortest interval setting that you are comfortable with and increase as needed.

- **Report Groupwise Sync Errors** – Sends an email alert when a GroupWise synchronization experiences an error.
- **Report RAID Errors** – Sends an email alert as soon as any RAID errors are encountered.

  > These errors immediately display to the *admin* user on the **BASIC > Status** page in the **Performance Statistics** section, irrespective of this setting.

- **Report High Storage Space Usage** – Sends an email alert when the storage space usage reaches the specified threshold.

  > The actual storage space data displays to the *admin* user on the **BASIC > Status** page in the **Performance Statistics** section as *Mail/Log Storage*, irrespective of this setting.

- **Report Automated Backup Errors** – Sends an email alert if an automated (scheduled) backup fails for any reason. To verify connectivity to the backup location, use the **Test Backup Server** on the **ADVANCED > Backup** page to receive immediate results (no emails are generated during testing).
- **Outbound SMTP Host (Smart Host), Outbound SMTP Port** – Your normal outbound SMTP host, or your Microsoft Exchange Server Smart Host, and the associated port. Click **Test SMTP Connection** to test the test the connection.

  > If your Smart Host accepts SMTP connections on a different port, this can be set in the TCP Port field.

SMB Export Options

The Barracuda Message Archiver can enable a local SMB/CIFS share called ***BarracudaMessageArchiverSmbPickup*** to be used to download .zip or .pst files from exports performed on the Search page. By default this share is not enabled, and exports must be downloaded from the **ADVANCED > Task Manager** page. In some cases, for instance large exports, using the web interface is not desirable and enabling the share can be helpful.

From the **ADVANCED > Administration** page, click on Help for more details on SMB Export.

Also see the Barracuda Networks Solution #00004903

Search Page Settings

Global settings for the **BASIC > Search** page. Each setting can be customized by account role: *Admin* , *Auditor* or *User* .

- **Display All Messages on Start** – Causes all available messages to display by default when bringing up the **BASIC > Search** page. Loading all available messages can take a significant amount of time, so disabling this setting allows faster access to enter and execute search commands. This option does **not** affect the behavior when a Saved Search is loaded from the **Saved Searches** tab.
- **Preserve Journal Wrappers** – Includes the journal envelope (which reflects all headers, including the BCC header) when exporting, downloading, or viewing the source of messages pulled from Microsoft Exchange journal accounts. These wrappers are generally not included when exporting or forwarding messages, but in some cases it may be desirable to keep this additional information.

  > This feature is not applicable to the user role.

- **Export Allowed** – Enables the **Export Selected** option in the **Tools** button of the **Search** page for the selected role.
- **Export All Search Results Allowed** – Enables the **Export All** option in the **Tools** button of the **Search** page for the selected role.
- **Forward Allowed** – Enables the **Forward Selected** option in the **Tools** button of the **Search** page for the selected role.
- **Forward All Search Results Allowed** – Enables the **Forward All** option in the **Tools** button of the Search page for the selected role.
- **"Tag All" Allowed** – Enables the "**Tag All**" option in the **Tools** button of the appropriate **Tags** tab for the selected role.

  > Tagging can only be performed from the **PSTs & Tags** tab for the *Admin* and *Auditor* roles, and the **Folders & Tags** tab for the *User* role. Tagging cannot be done from the **Standard** search tab, by any role.

- **Enable Preview Pane** – Allows the selected roles to use the **Preview Pane** from the Search page.

Secondary Authorization

Secondary Authorization allows you to require an additional password from both *Admins* and *Auditors* before executing any action that could expose message data, such as accessing the Search pages or the Audit Logs. Once Secondary Authentication is enabled and a password is set, that same password is also required for all subsequent changes to Secondary Authentication, including to the password itself.

- **Enable Secondary Authorization** – Causes certain potentially sensitive actions to require an additional password to be entered before execution. When set to **Yes**, the password fields display.

System Reload/Shutdown

- **Shutdown** – Shuts down and powers off the Barracuda Message Archiver.
- **Restart** – Reboots the Barracuda Message Archiver.
- **Reload** – Re-applies the system configuration. Will also re-initialize the message database to allow the most recent (within the past 30 minutes) messages archived on the Barracuda Message Archiver, to be included in searches.

Step 5: Understanding Message Archiving Concepts

> This article refers to the Barracuda Message Archiver release 3.1 or higher, except where noted.

Once you configure your administrative settings, review the following Message Archiving concepts.

In this article:

- Policy Monitoring
- Auditing
- Stubbing
- Attachment Parsing

- Exporting Messages
- Alias Unification
- Archived Data Backup

Policy Monitoring

Many organizations need to keep track of organizational policy violations, and to be alerted when violations occur. Policies can include defining when it is acceptable to send messages containing executable files or any inappropriate content (usually never); identifying how often messages containing references to forbidden topics are sent (especially when litigation is expected); and when certain email recipients can be contacted (excessive personal emails during business hours).

The Barracuda Message Archiver includes a set of standard policies that are updated regularly via Energize Updates, and allows you to easily create your own policies to fit your specific organization environment. You can configure alerts to go out whenever a policy violation is detected, and reports are available to summarize new policy violations and to detect any that are found amongst the messages stored in the archive.

Auditing

Organizations frequently use outside firms to perform an audit of company records. With the Barracuda Message Archiver, you can provide an independent auditor complete access to all data. Using the Auditor role, there is no need to add the user directly to the official directory structure, nor is there need to assign the user administrator-level privileges to the entire network.

Specific individuals or accounts can be assigned special audit privileges on the Barracuda Message Archiver including the ability to create and monitor policies, and to flag messages as needed.

Stubbing

Stubbing refers to the replacement of the often sizable attachments in messages with "stubs" that contain a link from which an attachment can be retrieved, thus eliminating the need to store attachments on the mail server where they take up valuable disk space. Messages that have stubs in place of the actual attachment can still be read, forwarded, and otherwise acted upon in the same manner as messages with embedded attachments.

The Barracuda Message Archiver supports stubbing with Microsoft Exchange mail servers, and offers an add-in for Microsoft Outlook that allows users to easily stub or unstub their own messages containing attachments.

Attachment Parsing

Parsing is the process of analyzing and indexing searchable text. In addition to message parsing, the Barracuda Message Archiver parses attachments.

Attachment Types

To make attachment content available to the Search page, the Barracuda Message Archiver parses the following types of attachments:

- Text and HTML
- PDF
- Microsoft Word, PowerPoint, and Excel
- Social Media content sent from the Barracuda Web Filter
- Common compression formats including .**zip**, .**tar**, .**gzip**, .**lha**, .**zoo**, .**arc**, .**arj**, and .**rar** can be unpacked and the compressed document examined even if the compressed content is made up of multiple formats

Because attachments can be very large, total parsable attachment text is limited based on the Barracuda Message Archiver model as shown in the following table:

Model	Attachment Parsing Cutoff [(1)]
150	348k = 174 pages of text
350	384k = 192 pages of text
450	512k = 250 pages of text
650	1MB = 500 pages of text

850	2MB = 1000 pages of text
950	4MB = 2000 pages of text
1050	6MB = 3000 pages of text
Note: (1) The full attachment is always archived.	

Attachment parsing limits apply only to those areas within an attachment that are searchable. For example, a 10MB attachment generally contains elements that are not parsable text, for example, graphics, file metadata, formatting, etc. Such attachments may ultimately contain only 100KB of parsable text and will be indexed in their entirety by all Barracuda Message Archiver models.

Example
If you have a model 450 (512k attachment parsing limit), and someone sends you an extremely large PowerPoint presentation containing 5 lines of text per slide and numerous graphics and animations, you can estimate that each slide takes up approximately ¼ page of text. In this example, the Barracuda Message Archiver parses and indexes the text content of a 1000-slide PowerPoint presentation.

Note that the entire presentation is always stored, and if the presentation exceeds 1000 slides, you can search and match content from the first 1000 slides within that presentation. This is true whether you are journaling all content or if you are simply stubbing attachments.

Exporting Messages

Messages found to be in violation of organizational policy often need to be gathered together for easy presentation. Once a search has located the messages you want to export, the Barracuda Message Archiver can export either a **.zip** file containing **.eml** versions of the selected messages, or a **.pst** file. Additionally, in firmware release 3.5 and higher, you can select to download to a Copy account. For details, go to the **BASIC > Search** page in the web interface, and click the **Help** button.

Alias Unification

Each user typically has only one account on the email server, but may have multiple email addresses (usually variations on their initials and names) that they also receive. These aliases are resolved by the email server using protocols such as LDAP so that messages addressed to an alias are actually delivered to the appropriate email account.

The Barracuda Message Archiver unifies the primary account with all of its known aliases so that a user has archive access to all messages received by that user regardless of the "Send To" address on the message.

Archived Data Backup

The Message Store of the Barracuda Message Archiver should be backed up just as you would back up your data on any other data storage device. For details, refer to the following articles based on your firmware version:

- Firmware version 3.2 and earlier – How to Back Up Your Barracuda Message Archiver
- Firmware version 3.5 and higher – How to Back Up Your Archived Data

Security

Best Practices for Securing your Barracuda Message Archiver

- Understanding Compliance
- How to Create Policy-Based Security
- How to Define Archived Message Retention Policies Based on Saved Searches

- How to Secure Network Access

Understanding Compliance

This article refers to the Barracuda Message Archiver release 3.1 or higher.

The Barracuda Message Archiver provides everything an organization needs to comply with government regulations in an easy to install and administer plug-and-play hardware solution. The Barracuda Message Archiver stores and indexes all email for easy search and retrieval by both regular users and third-party auditors. Backed by Energize Updates, delivered by Barracuda Central, the Barracuda Message Archiver receives automatic updates to its extensive library of virus and policy definitions to enable enhanced monitoring of compliance and corporate guidelines as well as document file format updates needed to decode content within email attachments.

The Barracuda Message Archiver features an easy-to-use web user interface, creating an intuitive and cost-effective administration tool for the integrated hardware and software solution. The web user interface allows administrators to define, manage, and control corporate archiving settings and rules from a central location.

Related Articles

- Create Policy-Based Security
- Saved Search Retention Policies
- Auditor Role

The Barracuda Message Archiver provides:

- Litigation Support
- Storage Management
- Knowledge Management
- Compliance

Litigation Support

Litigation discovery involves all parties in a lawsuit and requires that all data or information relevant to the lawsuit be provided as requested by the court of law. The Barracuda Message Archiver stores and indexes all email for easy search and retrieval by both regular users and third-party auditors.

Storage Management

Not only does the volume of email messages continue to increase, the size of the average email itself is also on the rise. Due to the increased use of file attachments in email messages, the average email size can range between 22KB and 350KB. As such, the ability for an organization to adequately keep up with the storage demands of email can be costly. While storage solutions can be used to deal with the problem of email message growth in the short term, the Barracuda Message Archiver provides a more resourceful way of handling the issue over a longer period of time.

Knowledge Management

A company's email system contains a vast amount of vital corporate intelligence, some of which is not replicated in any other data or material. If email is lost or is not easily accessible, a company runs the risk of losing that intelligence. The Barracuda Message Archiver provides management tools essential to storing and controlling access to an organization's knowledge base.

Compliance

Compliance issues are perhaps the driving force behind the increase in demand for an email archiving solution. The sheer number of regulations requiring some form of email retention, as well as the more specific parameters of how the email should be stored and for how long, can be confusing for administrators.

Although many regulations exist and have varying requirements, compliance is based on three concepts:

- **Email permanence** – Email must be maintained in its original form without alteration or deletion
- **Email security** – Information must be protected against all threats including unauthorized access to the email as well as physical damage. This same concept applies to the process of legal discovery which often specifies who can access the email (i.e., legal teams) as well as safeguards against the destruction of hard copies of the data
- **Auditability** – Email must be easily accessible in a timely fashion by authorized personnel upon request

The following table summarizes some of the key government regulations, and indicates how the Barracuda Message Archiver, using a sophisticated set of logging, auditing, and management capabilities, can help organizations achieve compliance.

Regulatory Compliance

Regulation	Description	Barracuda Message Archiver Logging/Storage	Search/Alerts
Federal Rules of Civil Procedure (FRCP)	the FRCP sets rules for governing court procedures in managing civil suits in the United States district courts.	The Barracuda Message Archiver stores up to10 years worth of email through a combination of internal and external storage.	Email messages are fully indexed according to popular message fields including subject, sender/receiver, date, attachment, importance, and more. Custom policies can be set to alert when terms related to ongoing litigation are contained in emails and their attachments.
Sarbanes-Oxley (SOX)	The Sarbanes-Oxley Act of 2002 requires companies to implement policies and systems to monitor and prevent fraudulent activities.	The Barracuda Message Archiver stores up to 10 years worth of email through a combination of internal and external storage.	Email messages are fully indexed according to popular message fields including subject, sender/receiver, date, attachment, importance and more.
SEC/NASD	Firms in the financial services industries must adhere to strict sets of rules imposed by governing bodies.	The Barracuda Message Archiver stores up to 10 years worth of email through a combination of internal and external storage. The Barracuda Message Archiver also includes tamper-resistant safeguards to protect the integrity of the email archive.	Email messages are fully indexed according to popular message fields including subject, sender/receiver, date, attachment, importance and more. Reports can also be generated that log attempts to tamper with the archive storage.
Health Insurance Portability and Accountability Act (HIPAA)	HIPAA mandates all healthcare and insurance providers determine who has access to health information and ensure that such information remains inaccessible to unauthorized parties.	The Barracuda Message Archiver stores up to 10 years worth of email through a combination of internal and external storage.	Alerts can be customized to notify the administrator when a policy has been violated. Policy definitions included with Energize Updates will update the Barracuda Message Archiver's lexicon with the latest advances in health care industry.

How to Create Policy-Based Security

This article refers to the Barracuda Message Archiver release 3.1 or higher.

Data retention policies allow you to specify message retention policies and Saved-Search retention policies on the **POLICY > Retention** page. Retention policies are the only way to purge messages; data cannot be deleted directly by a user.

In this article:

- Global Retention Policy

- Saved-Search Retention Policy
- Litigation Holds

Retention Policies

By default, automated archived message purging on the Barracuda Message Archiver is disabled. If you enable this ability, the Global Retention Policy and any Saved-Search retention policies are run against all the archived messages once a week. If the age of a message exceeds the maximum age allowed by all Saved-Search retention policies that apply to the message, that message is permanently deleted from the Barracuda Message Archiver. The Global Retention Policy setting does not apply to any messages that match a Saved-Search retention policy.

To enable or disable the automatic message expiration capability:

- On the **POLICY > Retention** page, specify whether to **Allow automatic message deletion**.

Global Retention Policy

The Global Retention Policy applies to all archived messages. When retention policies are run against the archived messages once a week, any messages stored on the Barracuda Message Archiver that are older than this age are deleted *unless* they match an existing Saved Search policy.

To configure the Global Retention Policy:

1. On the **POLICY > Retention** page, set **Allow automatic message expiration** to **Yes**.
2. In the **Policy Length (Days)** field, enter the default maximum number of days to retain archived messages.
3. Click **Save Changes**.

Saved-Search Retention Policy

A Saved-Search retention policy enables you to automatically expire messages that match a particular set of content criteria defined in the **BASIC > Search** page. Use this feature to create exceptions to the global Retention Policy.

> Saved searches containing tags cannot be used in a Saved-Search retention policy and do not appear in the list of available Saved Searches.

To configure a Saved-Search retention policy:

1. Go to the Barracuda Message Archiver. Note the criteria specified by the Saved-Search on which this retention policy is to be based. If you need to create a saved search, go to the **BASIC > Search** page. After you create and saved a search, you can use it as part of a Saved-Search retention policy definition.
2. Verify **Allow automatic message expiration option** is set to **Yes**.
3. In the **Saved-Search Retention Policy** table, complete the following:
    a. In the **Policy Name** field, enter a name for the policy you are creating.
    b. In the **Saved Search** field, select the name of the saved search on which this retention policy is to be based.
    c. In the **Policy Length** field, enter the number of days to retain archived messages that match these search criteria.

    > If a message matches more than one Saved Search-based policy, then the message is kept according to the *longest* p olicy length. If it matches a Saved Search-based policy as well as the global policy, then the Saved Search policy takes precedence.

4. Click **Add**.

See How to Define Archived Message Retention Policies Based on Saved Searches for more information.

Litigation Holds

Litigation Holds are created by auditors to prevent messages that meet the criteria for a specific Saved-Search from being removed from the Barracuda Message Archiver. The system administrator must first **Enable Litigation Holds** before auditors are given the option to create Litigation Holds from the **Saved Searches** tab on the **BASIC > Search** page.

The following information about active Litigation Holds will be displayed here, visible only to the system administrator:

- **Auditor –** The account name of the Auditor who created the Litigation Hold
- **Saved Search** – The name of the Saved Search associated with this Litigation Hold
- **Hold End Date** – The date and time when this Litigation Hold expires

The system administrator can stop a Litigation Hold by clicking on the trashcan icon for the entry.

How to Define Archived Message Retention Policies Based on Saved Searches

This article refers to the Barracuda Message Archiver release 3.1 or higher.

Saved Search Retention Policies

You can define a retention policy based on a Saved Search to automatically delete archived messages from the Barracuda Message Archiver. Note that before you can create a Saved Search retention policy, you must create at least one Saved Search in the **BASIC > Search > Advanced Search** page.

Important
Litigation holds overwrite Saved Search and Global Retention Policies; a litigation hold may be for a defined period of time or indefinite.

Messages that match the specified Saved Search are permanently removed from the Barracuda Message Archiver when the age of the message exceeds the specified Saved Search policy length.

If you define multiple Saved Search retention policies, if the age of any message exceeds the maximum age allowed by all Saved Search retention policies that apply to the message, that message is permanently deleted form the Barracuda Message Archiver.

Because a Saved Search retention policy overrides the Global retention policy, Saved Search retention policies are useful when you want to create exceptions to a global retention policy.

Automating Message Purging

To run Saved Search retention policies against archived messages, go to the **POLICY > Retention** page, and turn on **Allow automatic message deletion**. Once enabled, the Saved Search policies are run against archived messages on a weekly basis each weekend.

Setting Up a Saved Search Retention Policy

1. Log in to the Barracuda Message Archiver, go to the **BASIC > Search** page, and in the **Standard** tab, click **Advanced**.
2. Enter the search criteria, and click **Save Search**.
3. Enter the **Search Name**, and click **OK**.
4. Go to the **POLICY > Retention** page, and enter the **Saved Search Retention Policy** details:
   - In the policy **Name** field, enter a name for the policy you are creating.
   - In the **Saved Search** field, select the name of the saved search on which this retention policy is to be based.
   - In the **Policy Length (Days)** field, enter the number of days to retain archived messages that match the Saved Search criteria.
5. Click **Add**.

Important
If a message matches more than one Saved Search-based policy, then the message is kept according to the *longest* policy length. If it matches a Saved Search-based policy as well as the global policy, then the Saved Search policy takes precedence.

How to Secure Network Access

This article refers to the Barracuda Message Archiver release 3.1 or higher.

To secure your Barracuda Message Archiver on your network, begin by locking down the user interface ports. Barracuda Networks recommends using the non-standard port 8000 for internal access to the web interface, which is configured on the **BASIC > Administration** page. From this page you can also further limit access to the web interface by IP address in the **Administrator/IP Range** section. If no IP address is specified in this field, then all systems are granted access with the correct administrator password.

You can secure external access to the Barracuda Message Archiver with the **Web Interface HTTPS/SSL Port** setting on the **ADVANCED > Secure Administration** page. The recommended port is 443 because it is a standard HTTPS/SSL port used for secure web browser communication, and the identity of the remotely connected server can be verified with significant confidence.

SSL Certificates

Limiting user interface access to HTTPS provides further security and can also be configured on the **ADVANCED > Secure Administration** page along with the use of SSL certificates. There are three types of SSL certificates to choose from:

- Default (Barracuda Networks);
- Private (self-signed);
- Trusted certificate - a certificate signed by a trusted certificate authority (CA).

Specific steps for configuring SSL certificates is described in the section Enabling SSL for Administrators and Users.

Track Changes to the Configuration and User Login Activities

The syslog function of the Barracuda Message Archiver provides two kinds of logs, capturing:

- User login activities and any configuration changes made on the device;
- Data related to mail traffic. This data is the same information as that used to build the Message Log in the Barracuda Message Archiver.

From the **ADVANCED > Syslog** page, use the **Monitor Syslog** button to view the mail syslog output.

Backup and Storage

Expansion Storage is available only on Barracuda Message Archivers shipped prior to May 15, 2013. See Storage Details for further information.

In this Section

- Storage Backup
- Storage Manager

Related Articles

- Configuration Backups

Storage Backup

This article refers to the Barracuda Message Archiver release 3.1 or higher.

In this article:

- Backup of Archives
  - NFS Shares
  - SMB Access
- Desktop Backups
- Automated Configuration Backups

The Message Store of the Barracuda Message Archiver should be backed up just as you would back up your data on any other data storage device. Data is stored on the share in files of about 1GB in size. *All files in all shares must be backed up.* Be aware that although you can back up the files, you must contact Barracuda Networks Technical Support in order to restore any of the data.

Backups can be saved to any FTP or SMB location to which the Barracuda Message Archiver has access. To create internal storage volume backups, you can enable Show Local Backup Options on the **ADVANCED > Backup** page to display the backup options.

Backup of Archives

In the **Backup of Archives** section, you can enable NFS or SMB access to the message store, and create local storage backups. For more information, refer to Archived Data Backup.

- For backups via SMB, the username used to connect to the published SMB share is always **smb**, but you can optionally specify a workgroup name and an access password.
- When publishing the data partition via NFS, please contact Barracuda Networks Technical Support for assistance in restricting access to the NSF share by IP address.

The Message Store can be made available as an NFS or SMB share on your network. Provide the following information to enable any share:

- **Back Up Archives via NFS** – Set to **Yes** to enable access to the Message Store as NFS shares.
- **Back Up Archives via SMB** – Set to **Yes** to enable SMB access to the Message Store.
- **Workgroup** – Enter the name of the Workgroup that the share is to be a part of.
- **Password** – Enter the password required to access the network share.

NFS Shares

The number of shares on the Barracuda Message Archiver can vary. All models will have share number 1, while higher model numbers may have additional shares. Possible share configurations include:

share numbers
1
1, 2
1, 2, 3, 4

Enabled NFS shares can be mounted as:
`host:/BMA-NFS-#`

where *host* is the hostname or IP address of your Barracuda Message Archiver, and # is the share number.

Users of NFS v4 must also include the option **-o vers=3** in the mount command.

Example:

If the IP address of your Barracuda Message Archiver is 192.168.1.10, to mount the second share you issue the command:
`mount -t nfs 192.168.1.10:/BMA-NFS-2 dir`
where *dir* is the path where the share is to be mounted.
Similarly, for NFS v4 users, use the command:
`mount -t nfs -o vers=3 192.168.1.10:/BMA-NFS-2 dir`

SMB Access

If SMB access to the Message Store is enabled, it can only be accessed by the username **smb** using the **Password** specified above.

SMB shares enabled for backing up the Message Store are *not* the same as the shares used for other purposes, such as importing **.pst** files. Refer to the **BASIC > Administration** page to enable SMB shares for other uses.

The number of shares on the Barracuda Message Archiver can vary. All models have share number 1, while higher model numbers may have additional shares. Here are the possible share configurations:

share numbers
1
1, 2
1, 2, 3, 4

Enabled SMB shares can be reached at:
`\\host\BMA-SMB-#`

where *host* is the hostname or IP address of your Barracuda Message Archiver, and # is the share number.

If you are already connected to another SMB share on your Barracuda Message Archiver, you may need to specify the host name instead of the IP address.

Example:

If the IP address of your Barracuda Message Archiver is 192.168.1.10, to connect to the second share use:
`\\192.168.1.10\BMA-SMB-2`

Desktop Backups

Backups can be made of the configuration of your Barracuda Message Archiver to a file on your local machine. These files can be used for backup purposes, as well as for uploading to another Barracuda Message Archiver running the same or higher firmware version. Backups can be created manually to be saved to your desktop as needed, or created automatically to be saved onto a storage server on a regular basis.

Select a file in the **Available Backups** table in the **Cloud-Based Configuration Backups** section, and then click **Backup** in the **Desktop Backup** section to initiate the creation of a configuration backup file to be saved locally. The default filename is in the format `BAR-MA-`*`serial-date`*`-Config_Backup.bak`, where:

- *`serial`* is the serial number of the unit
- *`date`* is the date and time the backup was initiated

> **Caution**
> A checksum is placed in each configuration text file to prevent accidental errors in the Barracuda Message Archiver configuration information. Any changes made to the file will cause the existing checksum to be incorrect, which prevents upload of the modified configuration file. Customers who want to manually edit a configuration file should contact Barracuda Networks Technical Support for the proper procedure.

Automated Configuration Backups

The settings in the **Automated Configuration Backups** section allow you to select the components you want to back up, specify the backup schedule, and determine how many backups to keep on the remote server.

To automatically generate backups, configure a location on a remote server where the backups are to be kept, and determine which backups should happen when. Each backup type is saved individually, even if they are scheduled to be created at the same date and time.

- **Server Type** – The type of server used to store the backup files. Options are **FTP** and**SMB (Windows Shared)**. Set to *Off* to temporarily disable automated backups without losing any configured data.
- **Server Name/IP** – The hostname (FQDN) or IP address of the backup server.

  > If you have selected **SMB** above and are using a Windows 2003 server, you must use the Windows netbios name and not an IP address in this field.

- **Port** – The port used to connect to the backup server. If left blank, the port number most commonly associated with the selected server type is used.
- **Username** – The username used to connect to the backup server. Generally a single, lowercase word with no symbols.
- **Password** – The password used with the username above. On save, this always displays as 14 filled circles, no matter the length of the actual password.
- **Folder/Path** – The full path to the folder or share that is to be mounted by the backup process. This is required in all cases.
- **Backup Schedule** – When to perform the backup. Changes to the backup schedule take effect after midnight, so even a modification made at 09:23 for a 15:00 backup does not kick in until the following day at 15:00.
- **Backups to Keep** – The number of backups to retain on the backup server. Older backups are automatically purged.

Click **Test Backup Server** to verify connectivity to your backup server once your access information is entered. Results display in a new browser window.

Understanding Archived Data Backup

This article refers to Barracuda Message Archiver firmware version 3.5 or higher.

In the event of a catastrophe, backed up data partition content can be quickly restored. Back up the raw email data including **.zip** files present on the data partition as well as data directories that house statistics, index, and other metadata snapshots the Barracuda Message Archiver generates for content.

Related Articles
• How to Back Up Your Archived Data

Important
While use of the Storage Manager/Mirror capability (**ADVANCED > Storage Manager** page) will push a real-time copy of raw emails to a customer data share, metadata snapshots are not mirrored. You must back up this content by connecting to the Barracuda Message Archiver's read-only SMB share. Metadata content is available for Mirroring in a future point release of the firmware.

To fully realize this restoration method, you must consistently back up the following:

- Raw Email data:
  - ***.zip** (1GB-sized message archives)
  - <*nnn*>/ (directory containing recently received emails, not yet merged into a **.zip**)
- Snapshots of Metadata:
  - FolderSync (snapshot of folderync data)
  - index (snapshot of archives of index metadata)
  - index_backup (snapshot of the entire index)
  - ldap_cache (snapshot of ldap group information)
  - log (snapshot of important system information)
  - postgres_backup (snapshot of system databases)

Because snapshots are performed nightly, in the event that data restoration is necessary, typically only raw emails arriving in the last day must be reprocessed.

How to Back Up Your Archived Data

This article refers to Barracuda Message Archiver firmware version 3.5 or higher.

In this article:

- Set Up Backups
- Set Up Archive Backup
- Access Enabled Share
- Restore Data Partition Content

Related Articles

- Understanding Archived Data Backup
- Backing Up Data Using an External Solution

Important
While use of the Storage Manager/Mirror capability (**ADVANCED > Storage Manager** page) will push a real-time copy of raw emails to a customer data share, metadata snapshots are not mirrored. You must back up this content by connecting to the Barracuda Message Archiver's read-only SMB share. Metadata content is available for Mirroring in a future point release of the firmware.

Set Up Backups

Use the following steps to set up Barracuda Message Archiver archive backup:

1. Log in to the Barracuda Message Archiver, and go to the **ADVANCED > Backups** page.
2. In the **Backup of Archives** section, set **Back Up Archives via SMB** to **Yes** to allow access to the message store as an SMB share.
3. Enter the **Workgroup** in which the Barracuda Message Archiver should appear.
4. Enter the **Password** for the username **smb** used to connect to the SMB share.
5. Click **Save Changes**.

Set Up Archive Backup

Log in to your Windows Network or Backup System such as the Barracuda Backup Server.

1. Log in to your network system.
2. Back up the following files and directories:

- Raw Email data:
  - ***.zip** (1GB-sized message archives)
  - *<nnn>*/ (directory containing recently received emails, not yet merged into a **.zip**)
- Snapshots of Metadata:
  - FolderSync (snapshot of folderync data)
  - index (snapshot of archives of index metadata)
  - index_backup (snapshot of the entire index)
  - ldap_cache (snapshot of ldap group information)
  - log (snapshot of important system information)
  - postgres_backup (snapshot of system databases)

Nightly Backups
Snapshots are performed nightly. Therefore, in the event that data restoration is necessary, typically, the only raw emails that must be reprocessed are those that arrived in the last day.

Access Enabled Share

To access the share after it is enabled, connect to **\\<*IP*>\BMA-SMB-<*sharenumber*>**

Restore Data Partition Content

To restore data partition content, contact Barracuda Networks Technical Support.

How to Back Up Your Barracuda Message Archiver

This article refers to the Barracuda Message Archiver release 3.1 or higher, except where noted.

Message Archiver models (excluding the 150) provide RAID storage to protect against physical drive failure. However, other environmental or catastrophic issues may occur that the built-in RAID redundancy cannot protect against.

For this reason, it is strongly recommended that the Barracuda Message Archiver administrator make use of the available mechanisms to back up the email data to an external location.

There are two methods for backing up the data partition on your Barracuda Message Archiver from within the web interface:

- **Option 1. Configure a Data Partition Mirror** – Create a mirror of the Barracuda Message Archiver data partition on an external network device.
- **Option 2. Message Store Backup** – The data partition of the Barracuda Message Archiver can be accessed by an external backup solution such as the Barracuda Backup Server.

Option 1. Configure a Data Partition Mirror

Firmware Release 3.5 and Higher
In firmware release 3.5 and higher, note that while use of the Storage Manager/Mirror capability (**ADVANCED > Storage Manager** page) will push a real-time copy of raw emails to a customer data share, metadata snapshots *are not mirrored*. You must back up this content by connecting to the Barracuda Message Archiver's read-only SMB share. Metadata content is available for Mirroring in a future point release of the firmware.

You can add additional storage volumes and enable mirroring for existing storage to provide redundancy of data. Configure a real-time mirror of the Barracuda Message Archiver's data partition through the **ADVANCED > Storage Manager** page.

You must disable anti-virus scan on the external share that is to be used as a mirror before adding the mirror share to the Barracuda Message Archiver mirror.

You can use any network share that supports the SMB/CIFS file sharing protocols as the mirror. Additionally, the Barracuda Message Archiver models 850 and higher have a dedicated hardware iSCSI adapter that can be integrated with any iSCSI storage-area network

(SAN).

Use the following steps to add the mirror share to your configured network share:

1. Log into the Barracuda Message Archiver as the administrator, and go to the **ADVANCED > Storage Manager** page.

> **New Group**
> Note that you can select the default group, or click **Add New Group** to create a new storage group.

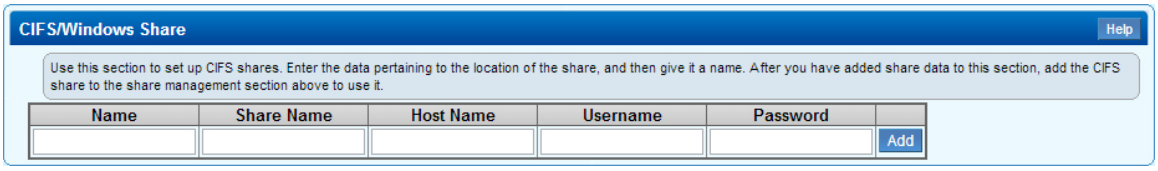
2. If you have an iSCSI or CIFS/Windows share already set up, complete the following step, otherwise go to step 3:

   a. Select the share from the drop-down menu, and enter the associated details.

   b. Click **Add Mirror**.

3. If you do not have an iSCSI or CIFS/Windows share already set up, complete the following steps:

   a. In the **Group** table, click **Add Mirror**; the **CIFS/Windows Share** section displays at the bottom of the page:


CIFS/Windows Share
Help
Use this section to set up CIFS shares. Enter the data pertaining to the location of the share, and then give it a name. After you have added share data to this section, add the CIFS share to the share management section above to use it.
Name
Share Name
Host Name
Username
Password
Add

   b. Enter the share details, and click **Add**.

   c. In the **Group** table, select the share you want to use to back up the data from the drop-down menu.

> Once you click **Add Mirror**, the Barracuda Message Archiver synchronizes the data on the existing share with the mirror share. During this sync, the Barracuda Message Archiver's Storage Manager may be unavailable for use, but will continue to archive mail. Note that a mirror share can only be added to internal shares.

For more information, refer to Storage Manager, or log into your Barracuda Message Archiver, go to the **ADVANCED > Storage Manager** page, and click the **Help** button.

Option 2. Back up the Data Partition Using an External Solution

You can back up archives using your existing backup solution, such as Barracuda Backup, via SMB access to the Barracuda Message Archiver's data partition.

> The Barracuda Message Archiver provides authenticated read-only access to the internal data partition via CIFS.

To do so,

1. Log into the Barracuda Message Archiver as the administrator, and go to the **ADVANCED > Backup** page.
2. In the **Backup of Archives** section, set **Back Up Archives via SMB** to *Yes* to allow access to the message store as an SMB share.
3. Set a workgroup name and password to connect to the SMB share; note that the SMB share username is always **smb**.
4. Click **Save** to save your settings.

On the external backup solution, connect to the Barracuda Message Archiver using SMB, and back up your data. The Barracuda Message Archiver shares are published as:
< *IP* > :/BMA-SMB -< *sharenumber* >

To back up the Barracuda Message Archiver using Barracuda Backup,

> **Firmware Version 5.1 or Higher**
> The following steps refer to Barracuda Backup firmware version 5.1 or higher.

1. Log in to Barracuda Backup as the Administrator, and go to the **BACKUP > Sources** page.

2. Click **Add Computer**. In the **Add Computer** page, enter a computer description and enter the IP address or fully qualified domain name in the **Computer Name** field.
3. From the **Computer Type** drop-down menu, select *Microsoft Windows*.
4. Set **Enable File Share Backups**; type `smb` as the **Username**, and enter the password you set up on the **ADVANCED > Backup** page in the Barracuda Message Archiver web interface.
5. Click **Test Credentials** to verify access to the file share.
6. Click **Save** at the top of the page.
7. In the **Add Data Source** page, from the **Data Type** drop-down menu, select **File Share - CIFS**.
8. Verify **Enable Backups** is turned **On**.
9. In the **File Share Information** section, enter *BMA-SMB* as the Share Name, and click **Test Share**.
10. In the **Folder Selection** section, specify which folders you want to back up.
11. To replicate to the cloud, turn on **Replicate to Barracuda Cloud Storage**.
12. Click **Save** to save your configuration and add the data source.
13. Go to the **BACKUP > Schedules** page, and add a schedule for the SMB share.

For more information, go to the go to the **ADVANCED > Backup** page in the Barracuda Message Archiver, and click the **Help** button.

Configuring a Data Partition Mirror

This article refers to the Barracuda Message Archiver release 3.1 or higher, except where noted.

Message Archiver models (excluding model 150) provide RAID storage to protect against physical drive failure. However, other environmental or catastrophic issues may occur that the built-in RAID redundancy cannot protect against.

For this reason, it is strongly recommended that the Barracuda Message Archiver administrator make use of the available mechanisms to back up the email data to an external location.

You can add additional storage volumes and enable mirroring for existing storage to provide redundancy of data. Configure a real-time mirror of the Barracuda Message Archiver's data partition through the **ADVANCED > Storage Manager** page.

You must disable anti-virus scan on the external share that is to be used as a mirror before adding the mirror share to the Barracuda Message Archiver mirror.

You can use any network share that supports the SMB/CIFS file sharing protocols as the mirror. Additionally, the Barracuda Message Archiver models 850 and higher have a dedicated hardware iSCSI adapter that can be integrated with any iSCSI storage-area network (SAN).

Use the following steps to add the mirror share to your configured network share:

Firmware Release 3.5 and Higher
In firmware release 3.5 and higher, note that while use of the Storage Manager/Mirror capability (**ADVANCED > Storage Manager** page) will push a real-time copy of raw emails to a customer data share, metadata snapshots *are not mirrored*. You must back up this content by connecting to the Barracuda Message Archiver's read-only SMB share. Metadata content is available for Mirroring in a future point release of the firmware.

1. Log into the Barracuda Message Archiver as the administrator, and go to the **ADVANCED > Storage Manager** page.

New Group
Note that you can select the default group, or click **Add New Group** to create a new storage group.

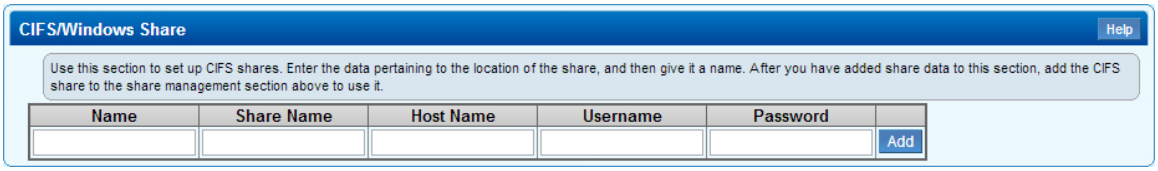
2. If you have an iSCSI or CIFS/Windows share already set up, complete the following step, otherwise go to step 3:

   a. Select the desired share from the drop-down menu, and enter the associated details.

   b. Click **Add Mirror**.

3. If you do not have an iSCSI or CIFS/Windows share already set up, complete the following steps:

a. In the **Group** table, click **Add Mirror**; the **CIFS/Windows Share** section displays at the bottom of the page:


CIFS/Windows Share
Help
Use this section to set up CIFS shares. Enter the data pertaining to the location of the share, and then give it a name. After you have added share data to this section, add the CIFS share to the share management section above to use it.
Name
Share Name
Host Name
Username
Password
Add

b. Enter the share details, and click **Add**.

c. In the **Group** table, from the drop-down menu, select the share you want to use to back up the data.

> Once you click **Add Mirror**, the Barracuda Message Archiver synchronizes the data on the existing share with the mirror share. During this sync, the Barracuda Message Archiver's Storage Manager may be unavailable for use, but will continue to archive mail. Note that a mirror share can only be added to internal shares.

For more information, refer to Storage Manager, or log into your Barracuda Message Archiver, go to the **ADVANCED > Storage Manager** page, and click the **Help** button.

Backing Up the Data Partition Using an External Solution

This article refers to the Barracuda Message Archiver release 3.1 or higher.

In this article:

- Drive Partitions
- Data Partition Backup
- Barracuda Backup

Related Articles

- Storage Manager
- Archived Data Backup

> Message Archiver models (excluding model 150) provide RAID storage to protect against physical drive failure. However, other environmental or catastrophic issues may occur that the built-in RAID redundancy cannot protect against.
>
> For this reason, it is strongly recommended that the Barracuda Message Archiver administrator make use of the available mechanisms to back up the email data to an external location.

Use the steps in this article to back up the Barracuda Message Archiver message store using an external solution.

Drive Partitions

The number of shares on the Barracuda Message Archiver can vary. All models have share number 1, while higher model numbers may have additional shares. If there are additional shares, the share BMA_SMB contains these other directories. For example, a Barracuda Message Archiver 350 has one drive partition, **BMA-SMB-1**, which you would select to back up.

Here are the possible share configurations:

share numbers
1
1, 2
1, 2, 3, 4

Data Partition Backup

You can back up archives using your existing backup solution, such as Barracuda Backup, via SMB access to the

Barracuda Message Archiver's data partition.

> The Barracuda Message Archiver provides authenticated read-only access to the internal data partition via CIFS.

To do so,

1. Log in to the Barracuda Message Archiver as the administrator, and go to the **ADVANCED > Backup** page.
2. In the **Backup of Archives** section, set **Back Up Archives via SMB** to **Yes** to allow access to the message store as an SMB share.
3. Set a workgroup name and password to connect to the SMB share; note that the SMB share username is always **smb**.
4. Click **Save** to save your settings.

On the external backup solution, connect to the Barracuda Message Archiver using SMB, and back up your data. The Barracuda Message Archiver shares are published as: *IP*:/BMA-SMB-*sharenumber*

Barracuda Backup

To back up the Barracuda Message Archiver using Barracuda Backup,

> **Firmware Version 5.1 or Higher**
> The following steps refer to Barracuda Backup firmware version 5.1 or higher.

1. Log in to Barracuda Backup as the Administrator, and go to the **BACKUP > Sources** page.
2. Click **Add Computer**. In the **Add Computer** page, enter a computer description and enter the IP address or fully qualified domain name in the **Computer Name** field.
3. From the **Computer Type** drop-down menu, select **Microsoft Windows**.
4. Set **Enable File Share Backups** to **On**; enter **smb** as the **Username**, and enter the password you set up on the **ADVANCED > Backup** page in the Barracuda Message Archiver web interface.
5. Click **Test Credentials** to verify access to the file share.
6. Click **Save** at the top of the page.
7. In the **Add Data Source** page, from the **Data Type** drop-down menu, select **File Share - CIFS**.
8. Verify **Enable Backups** is turned **On**.
9. In the **File Share Information** section, enter **BMA-SMB** as the Share Name, and click **Test Share**.
10. In the **Folder Selection** section, specify which folders you want to back up.
11. To replicate to the cloud, turn on **Replicate to Barracuda Cloud Storage**.
12. Click **Save** to save your configuration and add the data source.
13. Go to the **BACKUP > Schedules** page, and add a schedule for the SMB share.

> For more information, go to the go to the **ADVANCED > Backup** page in the Barracuda Message Archiver, and click the **Help** button.

Storage Manager

This article refers to the Barracuda Message Archiver release 3.1 or higher.

Most of the controls needed to manage both the internal and external storage volumes are on the **ADVANCED > Storage Manager** page. For storage capacity details by model, refer to the Barracuda Message Archiver Datasheet.

Related Articles

- Storage Backup
- Configuration Management & Access

Additional Resources

- Barracuda Networks KB Solution #0000 2671
- Barracuda Message Archiver Datasheet

> Expansion Storage is available only on Barracuda Message Archivers shipped prior to May 15, 2013. See Storage Details for further

information.

Mirroring

Enabling storage data mirroring provides data redundancy for added protection against corruption of the actual hardware, while reducing overall drive capacity. Note that you must disable anti-virus scan on mirror shares before adding those shares to a group on the **ADVANCED >Storage Manager** page.

You must disable anti-virus scan on mirror shares and rollover storage before adding shares to a group.

Email Notifications

All notification emails regarding storage maintenance, such as alerts for low storage space, are configured on the **BASIC > Administration** page.

Maintenance for any external storage that is added to the Barracuda Message Archiver can and should be performed as you would for any other data storage device.

Storage Details

Storage Details
Beginning May 15th 2013, internal storage capacity on Barracuda Message Archiver models 350 through 1050 has been doubled compared to previous-generation hardware. As part of this change, the extended storage expansion feature had been deprecated for these models. Units that were shipped prior to this change will continue to have this feature available.

To learn more about this change and the Barracuda Hardware Refresh program, please contact your Barracuda sales representative or authorized reseller.

Accounts, Roles, and Email Aliases

In this Section

- How to Manage User Accounts and Roles
- Understanding Email Aliases
- Audit Log Filtering
- Adding LDAP Users

How to Manage User Accounts and Roles

This article refers to the Barracuda Message Archiver release 3.1 or higher.

In this article:

- User Accounts
- User Roles
- Add Users
- Edit Users

User Accounts

There are two types of user accounts on the Barracuda Message Archiver:

- **Local Accounts** – These accounts reside only on the Barracuda Message Archiver and are created from the **USERS > User Add/Update** page in the administration interface.
- **LDAP Accounts** – These accounts reside in your LDAP directory. Once LDAP is configured on the Barracuda Message Archiver, users can log in using their regular network credentials to view and create flags for messages in their personal archive.

User Roles

Local Accounts are created with one of 3 Roles:

- **User** – Able only to view messages accessible to the account, either because the username for the account is also that of the sender or recipient of a message, or because it has been given explicit access to view an email address via Alias Linking.
- **Auditor** – Able to create and activate policies, and view, search, and export any messages to/from the domains to which they have access. To create a "Domain Auditor" (an auditor with access to only a subset of the domains on your Barracuda Message Archiver), set the role to Auditor and specify at least one domain. If no domains are specified, then all messages in the entire Barracuda Message Archiver are accessible. No auditor account has access to any system or network configuration information on the Barracuda Message Archiver.
- **IT Admin** – Able only to modify system and network configuration settings, and has no access to policies or any messages on the Barracuda Message Archiver.
- **Admin** – Able to view all items from any user, not just those listed for the account. Also able to create and activate policies, and can make other system or network changes.

The assigned Role can be changed at a later date from the **USERS > Local Accounts** page, but only the last assigned Role is active.

Add Users

Use the following steps to create a new user account:

1. Go to the **USERS > User Add/Update** page.
2. Enter the user's email address and specify whether to use the email address as the account name.
3. Click **Populate** to retrieve all aliases associated with the LDAP for the entered email address; note that you must configure an LDAP server on the **USERS > Directory Services** page to use this feature.
4. Enter the account password and select the user role for the account.
5. If you select the user role 'Auditor' enter the following additional details:
    - Enter a domain for which the auditor can view messages and other Outlook items, and click **Add.** Any messages that includes an email address in the listed domains in either the **From**, **To**, or **CC/Bcc** areas, or any items that belong to a user in the specified domains, display in search results. To allow the auditor to view all items from all domains, leave this field blank.
    - In the **Saved Search** drop-down menu, select a defined Saved-Search to automatically apply to all searches performed by this auditor. Note that the parameters in the Saved Search take precedence over any domain limitations that may be specified above, as well as over any attempts by the auditor to *Search As* any other account.

Edit Users

Use the following steps to modify user settings:

1. Go to the **USERS > Local Accounts** page:
    a. Click **Delete** to remove an account.
    b. Click **Edit** to modify the user; the **USERS > User Account Create/Update** page displays.
2. Update the user settings, and click **Save Changes**.

Auditor Role

The Auditor is able to create and activate policies, create litigation holds, and view, search, and export any messages to/from the domains to which they have access.

In this Section

- Viewing and Searching Messages - Auditor
- Saved Searches and Litigation Holds - Auditor
- Policy Alerts - Auditor
- Message Actions - Auditor

Viewing and Searching Messages - Auditor

This article refers to the Barracuda Message Archiver release 3.1 or higher.

In this article:

- Message Search
- Viewing a Message

- Executing a Search
  - Basic Search
  - Advanced Search

Related Articles

- Auditor Role
- Manage User Accounts/Roles
- Accounts, Roles & Email Aliases
- Advanced Search Options

Message Search

Searches are the main tools for the Barracuda Message Archiver, and can be made on virtually every aspect of a message including:

- message body content
- recipients and senders
- attachment type and content
- date

Searches can only be made over messages to which the Auditor has read access, so privacy is always preserved. Use the **Basic Search** page for quick one-time searches, or go to the **Advanced Search** page for a full array of search options including complex search queries and the ability to save searches. Saved Searches are the basis for Policy Alerts, used by Auditors and administrators to monitor compliance, and Retention Policies, to purge messages from the Barracuda Message Archiver that are older than a specified date.

Viewing a Message

The **BASIC > Search** page of Barracuda Message Archiver initially displays a list of the archived messages that are accessible to the viewing account. The Search page displays basic information about a message such as senders and recipients, date, subject, and size. You can view the contents of a message in one of two ways:

- the Preview Pane
- the Message Details window

> **Auditor Role**
> The Auditor role can be configured to have access to all mail, or to mail that meets specific patterns configured by the Administrator. See your Barracuda Message Archiver Administrator for details on your specific setup.

A single click on any message in the Search results sends it to the embedded Preview Pane for viewing. Double-click on a message to view it in a separate Message Details popup window. Both methods offer the ability to view the message as the sender intended for it to be viewed, as well as the underlying message source code. You can also select the character set to use for a particular message which can be especially useful when viewing a poorly formatted message that does not declare an appropriate charset. You can download each viewable message to your desktop as an .eml file.

Executing a Search

Searches can be executed from either the Basic Search or the Advanced Search pages. Both modes are available to all users who have the ability to search through messages, but only the Advanced Search page offers the ability to perform complex queries and create a Saved Search for use in Policy Alerts and Retention Policies.

Basic Search

The Basic Search interface accepts a word or phrase on which to search, and returns all available messages that contain the specified text in either the header or message body. This mode is useful when searching for that handful of emails to or from someone on a specific topic, or when looking for any message that contains a particular phrase. These are one-time searches as these cannot be saved for later use.

Advanced Search

You can perform more complex searches from the Advanced Search interface. This mode offers the ability to combine and negate multiple search parameters, save a particular combination of search parameters for future use, and execute any such Saved Search. You can search for messages in a variety of ways including:

- specifying a Natural Language or keyword expression as the search string
- limiting the scope of a search to specific parts of a message

- identifying messages that have a specific attribute, such as an attachment or an image
- restricting the search base to outbound, inbound, or internal messages only
- going only through those sent to or from specific email addresses, or those sent between specific dates

See Advanced Search Options for more information.

Saved Searches and Litigation Holds - Auditor

This article refers to the Barracuda Message Archiver release 3.1 or higher.

In this article:

- Saved Searches
- Litigation Holds

Related Articles

- Auditor Role
- User Accounts/Roles
- Accounts, Roles & Email Aliases

Saved Searches

Once you have designed a search from the **Advanced Search** page that locates the desired messages, you can save and name the search for re-execution at a later time. A list of all such Saved Searches and their definitions are available on the **POLICY > Alerts** page and each one can be performed from that page as well as the **Advanced Search** page.

Any changes to a Saved Search must be done from the Advanced Search page by running the Search in question, making the desired changes, and saving the new criteria. Use a new name to create a new Saved Search, or use the existing name to overwrite the previous set of search criteria.

To receive an alert via email when a message that fits the parameters of a Saved Search is received by the Barracuda Message Archiver, Policy Alerts are required.

Litigation Holds

You can create Litigation Holds to prevent messages that meet the criteria for a specific Saved Search from being removed from the Barracuda Message Archiver.

The system administrator must first **Enable Litigation Holds** on the **POLICY > Retention** page before an auditor can create Litigation Holds from the **Saved Searches** tab on the **BASIC > Search** page.

To add a Litigation Hold,

1. Log into the Barracuda Message Archiver as an auditor, go to the **BASIC > Search** page, and click the **Standard** tab.
2. Click **Advanced**, enter your search criteria, and click **Search**.
3. When the search results return, click **Save Search**, enter the **Search Name**, and click **OK**.
4. Click the **Saved Searches** tab, and in the **Actions** column for the selected Saved Search, click **Apply Litigation Hold**.
5. In the **Apply Litigation Hold** dialog, specify the **Hold End Date** as either:
    - Indefinite–Content that matches the Saved Search is retained until the Litigation Hold is cancelled
    - Specific Date–Enter the expiration date

Policy Alerts - Auditor

This article refers to the Barracuda Message Archiver release 3.1 or higher.

Policy Alerts are notifications that go out automatically whenever a message meeting specified criteria is detected entering the Barracuda Message Archiver based on a Saved Search.

Related Articles
• How to Set Up Saved Searches • Auditing Role • Accounts, Roles & Email Aliases

Creating Custom Policy Alerts

Use the following steps to create a new custom Policy Alert:

1. Log in to the Barracuda Message Archiver as an auditor, go to the **BASIC > Search** page, and click **Advanced**.
2. Enter the criteria for the policy. Click the **+** (plus) symbol to add additional search parameters, and click **AND/OR** to further clarify the search criteria.
3. Click **Search** to execute the search and verify the results. Click **Save Search**,enter a saved search name, and then click **OK**.
4. Go to the **POLICY > Alerts** page. Enter the **Policy Name**, and select the **Saved Search** from the drop-down menu.
5. Enter your email address to receive email alerts when a message meeting the Saved Search criteria is detected, and select the **Alert Frequency**.
6. If you want the policy to display in the **Policy Statistics** section on the **BASIC > Status** page, turn on **Dashboard**.
7. Click **Add**.

Message Actions - Auditor

This article refers to the Barracuda Message Archiver release 3.1 or higher.

In this article:

- Exporting Messages
- Forwarding Messages
- Tagging Messages

Related Articles
• Message Actions • User Accounts/Roles • Accounts, Roles & Email Aliases

The Barracuda Message Archiver allows you to easily collect messages for exporting or forwarding, and to add tags to messages for future re-identification if desired. You can control whether any or all of these actions are available to users on the **BASIC > Administration** page, in the **Search Page Settings** section.

Messages journaled directly from Microsoft Exchange have additional hidden information, such as bcc recipients and other SMTP data. End-users do not have access to this information; however, for compliance reasons you may want to include this hidden information when messages are exported or forwarded by the administrator or auditor. The **Preserve Journal Wrappers** setting, also in the **Search Page Settings** section, causes the body of an exported or forwarded message to consist of the complete envelope information, with the actual contents of the email turned into an attachment to the message.

Exporting Messages

Once a search is executed and the results are listed in the **BASIC > Search** page, you can choose to export one or more of these messages to a .pst or .zip file.

To export one or more messages, select the desired item(s) from the message list using Shift- or Ctrl-click to select multiple messages. Click on **Tools** located at the top of the message list, and click **Export Messages**. In the window select the desired action and export method. The desired messages are gathered into a single .pst or .zip file, and are available for download by any administrator from the **Tasks** tab in the **BASIC > Search** page.

Forwarding Messages

Once a search is executed and the results listed in the **BASIC > Search** page, you can specify one or more of these messages to be forwarded to a desired list of recipients.

To forward one or more messages, select the desired item(s) from the message list using shift- or ctrl-click to select multiple messages. Click on **Tools** located at the top of the message list, and select the desired action. A pop-up dialog prompts you for the email addresses of those users that are to receive the selected messages; use semi-colons to separate multiple email addresses.

Tagging Messages

Tag messages to easily identify any messages for future use. Tags can be any text, and can be accessed only by the account that created them.

To tag one or more messages, execute a search in the **BASIC > Search** page, and select the desired item(s) from the message list using Shift- or Ctrl-click to select multiple messages. Click **PSTs & Tags**, click on **Tools** located at the top of the message list, and select the desired Tag action. A pop-up dialog prompts you for the tag text. Tags can then be used as search criteria, allowing you to easily retrieve these messages at a later time.

Understanding Email Aliases

This article refers to the Barracuda Message Archiver release 3.1 or higher.

In this article:

- Group Membership
- Alias Linking
  - To list aliases for a new account
  - To list aliases for an existing account
- Discovery Option for Alias-Based Search

Group Membership

Archived messages that are sent to a mailing group are visible in the personal message archive for every member of that group. For example, if **csmith@company.com**, **patjones@company.com**, and **bdavis@company.com** are all members of **sales@company.com**, then any message that is sent to **sales@company.com** is available in the archives of all three users.

To enable this ability, you must be using an Active Directory or LDAP server, and the lists must reside on those servers.

Alias Linking

LDAP users often have one primary email address that is their user account name along with several aliases for convenience. For example, **csmith@company.com** might also receive messages as **chris.smith@company.com**, **chris@company.com**, and **c_smith@company.com**. For organizations that use LDAP, messages sent to any alias are also accessible from the primary user account on the Barracuda Message Archiver.

In addition, you can create a local user account on the Barracuda Message Archiver that has access to archived messages for multiple users. For example, you would like a single user account to be able to see emails for **chris.smith@company.com**, **pat.jones@company.com**, and **alex.pierce@company.com**, in addition to **the_boss@company.com**. To do so, create a local account on the Barracuda Message Archiver (for example, "local_boss"), and list as aliases the email addresses to which that account is to have access.

To list aliases for a new account

1. Go to the **USERS > User Add/Update** page.
2. Enter the new user **Email Address**, and specify whether the email is to be used as the account name.
3. Next to **Retrieve user Aliases from LDAP**, click **Populate**; the **User Aliases** field populates with all user aliases associated from the LDAP for the specified email address.
4. Click **Save Changes** to save the list of aliases for that user. This account is added to the **USERS > Local Accounts** page including its aliases.

To list aliases for an existing account

1. Go to the **USERS > Local Accounts** page.
2. Click **Edit** for the primary user account; the **USERS > User Add/Update** page displays.
3. Next to **Retrieve user Aliases from LDAP**, click **Populate**; the **User Aliases** field populates with all user aliases associated from the

LDAP for the specified email address.

4. Click **Save Changes** to save the list of aliases for that user. The aliases are added to the **Aliases** field for this user in the **USERS > Local Accounts** page.

Discovery Option for Alias-Based Search

When conducting an Advanced Search, you can search on all aliases associated with an LDAP for a specified email address using "Discovery". This option searches for all items sent to or received by any email alias, address or account associated with specified email addresses, as resolved against the LDAP servers identified on the **USERS > Directory Services** page. The email address specified here is expanded to include all of the entries returned by LDAP, and each email address in the resulting list is searched for in the **From**, **To**, **Cc** and **Bcc** fields.

> Email addresses must be completely formed, e.g., **username@example.com**.

To search on all aliases associated with an LDAP:

1. On the **BASIC > Search > Advanced** page, select **All** from the first drop-down menu, and select **Discovery** from the second drop-down menu.
2. Select **'**contains' and enter the user's email address.
3. Click **Search**.
4. To view all associated email addresses, click the alias icon ( ).

Audit Log Filtering

> This article refers to the Barracuda Message Archiver release 3.1 or higher, except where noted.
>
> The Audit Log is available to the admin and auditor roles.

In this article:

- Searching the Audit Log
- Audit Log Tools and Options

Related Articles

- Auditor Role
- User Accounts/Roles
- Accounts, Roles & Email Aliases

The **ADVANCED > Audit Log** page displays a list of all search-related activities that have been performed on the Barracuda Message Archiver. In this view you can browse through the list, or perform a search to filter on a subset of activities. You can filter by start/end dates, user name, and item type. Click on an activity to display the activity details in the **Details** pane.

Searching the Audit Log

Use the following steps to search the Audit Log:

1. Log in to the Barracuda Message Archiver, and go to the **ADVANCED > Audit Log** page. By default, all audit log records display.
2. Enter the desired search criteria, and then click **Search**.
3. The results pane displays those items matching the entered criteria. Information displayed for each record includes:
    a. **Date** - When the action occurred and was logged in the Audit Log.
    b. **User** - Which user performed this action. Some actions are performed by the Barracuda Message Archiver automatically, not actively by a specific user, displaying as user "System".
    c. **Type** - What type of action this record is for.
    d. **Detail** - Many audit log records contain information in addition to the date, user, and type. In some cases, a useful piece of this additional information is displayed in the **Detail** column, for instance to narrow down a broad action type.
4. To view additional information, click on an item. Details display in the right pane.

Audit Log Tools and Options

The Audit Log includes the following tools and options:

- **Page Navigation** - Click on the navigation arrows or type a number in the **Page** field to move through the Audit Log.
- **Refresh** ( ) Icon - Click the icon to update the page.

- **Export** *(available in firmware release 3.5 and higher only)* - Click **Export**, enter an email address to which to send a **.csv** file containing the selected audit logs in the dialog box, and click **OK**. Once the report generates, it is sent to the specified email address.
- **Tools** - Click to select the number of items to display per page and to specify the **Details Pane** location.

Adding LDAP Users

This article refers to Barracuda Message Archiver firmware 3.5 and higher.

Use the **USERS > LDAP Users Add/Update** page to associate an LDAP User or LDAP Group to a Barracuda Message Archiver role and list of email addresses. For example, you may want to prevent a user with the **Auditor** role from viewing specific user mailboxes.

Adding LDAP Users

Use the following steps to add an LDAP user or group:

1. Log in to the Barracuda Message Archiver, and go to the **USERS > LDAP Users Add/Update** page.
2. In the **LDAP User/Group** field, enter the LDAP User or Group name to which the permissions apply.

   The LDAP User/Group value can be any type of group such as a distribution group. Note that this cannot be an organizational unit (OU).
3. From the **Role** drop-down menu, select the role associated with the **LDAP User/Group** entry:
   - If you select the role **User**, specify whether to include or exclude mailbox addresses from the LDAP account:
     - In the **Include these Addresses** field, enter a mailbox address you want to make available to the specified LDAP account, and then click **Add**.
     - In the **Exclude these Addresses**, enter a mailbox address to hide from the specified LDAP account, and then click **Add**.
   - If you select the role **Auditor**, configure the permissions:
     - In the **Domains** field, enter a domain for which the auditor can view mail, and then click **Add**.
     - If you have defined Saved Searches in the **BASIC > Search** page, select a **Saved Search** from the drop-down menu to filter the auditor's search results.
     - In the **Exclude these Addresses**, enter a mailbox address to hide from the specified LDAP account, and then click **Add**.
   - If you select the role **IT ADMIN**, the specified **LDAP User/Group** account has IT Admin permissions only.
   - If you select the role **Admin**, enter a mailbox address to hide from the account in the **Exclude these Addresses**, and then click **Add**.
4. Click **Save Changes**.

In the **LDAP User/Group**, **Include these Addresses**, and **Exclude these Addresses** fields, enter the first three letters of a user or group name to display all matching values from which you can select.

LDAP User Include/Exclude Rules

This article refers to Barracuda Message Archiver firmware 3.5 and higher.

When adding LDAP users and LDAP groups to the Barracuda Message Archiver through the **USERS > LDAP Users Add/Update** page, inclusion/exclusion rules are analogous to whitelist/blacklist.

When a configured user runs a search on the **BASIC > Search** page, the following whitelist/blacklist rules are in place:

- Mail for addresses added to the **Exclude these Addresses** blacklist are NOT displayed unless the mail includes the user performing the search to assure that a user can always see their own mail.
- The **Exclude these Addresses** blacklist *always* takes precedence; addresses added to the **Include these Addresses** whitelist are searchable *unless* the **Exclude these Addresses** blacklist blocks the mail.
- Because a user with the Admin or Auditor role can by default view all mail, users set to these roles can only edit their **Exclude these Addresses** list.
- If a user is *not configured* and is a member of a group, then the blacklist/whitelist rules assigned to that group apply to that user. Additionally, if the unconfigured user is a member of multiple groups, then the privileges for all of those groups are merged and that user is assigned the *least privileged role* of those groups. This allows the Admin to apply blacklist/whitelist rules to all users of a distribution

group.

Exclude these Addresses
A user cannot run a **Search As User** Search on the **BASIC > Search** page on a user that is on their **Exclude these Addresses Exclusion Rules** blacklist.

Example Inclusion/Exclusion Rules

The following examples illustrates the inclusion/exclusion rules:

- **Example 1** - If Brian is not individually configured but is a member of the distribution group HR, then the Admin can set the blacklist/whitelist rules for the group HR, and Brian will use these settings when searching mail rather than seeing only his own mail.
- **Example 2** - If Josh is not individually configured but is a member of the distribution group HR which has an Auditor role, and Josh is also a member of the group Employees which has a User role, Josh has only the User role privileges when running a search.

Message Import, Stubbing, and Configuration Options

In this Section

- How to Import New Messages
- How to Import Historical Data
- Microsoft Exchange Server Integration
- Microsoft Exchange Server 2003, 2007, and 2010 Integration
- Understanding SMTP Forwarding and Trusted Servers
- Exchange Stubbing
- How to Retrieve Stubbed Messages in Shared Mailboxes
- Policy Alerts
- Retention Policies
- SMTP Proxy

Related Articles

- Understanding Email Encryption and Archival
- How to Set Up Email Encryption and Archival
- Archiving Encrypted Email Messages (Barracuda Spam Firewall)

How to Import New Messages

This article refers to the Barracuda Message Archiver release 3.1 or higher.

Depending on your network configuration, there are several ways in which the Barracuda Message Archiver can receive new messages (and other Microsoft Outlook items) for archiving.

Stubbing and Microsoft Exchange Import
For stubbing and Microsoft® Exchange imports initiated via the Barracuda Message Archiver user interface, there is a 100MB limit on file import.

In this Section

- How to Set Up Email Journaling
- How to Archive Microsoft Non-Email Items
- How to Synchronize Folders
- How to Import GroupWise Messages
- How to Import IBM Notes NSF Files

- How to Configure Your Barracuda Message Archiver to Act as an SMTP Proxy to Your Email Server

Related Information

For details on automatically importing, stubbing, and synchronizing Microsoft Exchange Server folder data, refer to the article Microsoft Exchange Server 2003, 2007 and 2010 Integration.

How to Set Up Email Journaling

This article refers to the Barracuda Message Archiver release 3.1 or higher.

This is the recommended method of sending messages to the Barracuda Message Archiver.

If your email server is capable of journaling, verify that it is set up and enabled per the directions for your particular email server. The Barracuda Message Archiver has been tested and verified to work with many different types of journaling email servers including (but not limited to):

- Microsoft Exchange
- IBM Lotus Notes/Domino
- IPSwitch Imail

Related Articles

- How to Set Up Microsoft Exchange 2007-2010 Envelope Journaling
- Configuring an SMTP Journal Account for Microsoft Exchange 2003
- IBM Lotus Notes/Domino IMAP Deployment

Additional Resources

- Barracuda Networks Knowledgebase Solution #00002528

Stubbing and Microsoft Exchange Import
For stubbing and Microsoft Exchange imports initiated via the Archiver user interface, there is a 100MB limit on file import.

To set up a Remote Journal Account deployment:

1. Configure your email server to journal messages as per the directions for your particular email server.
2. Go to the **MAIL SOURCES > Journal Accounts** page on the Barracuda Message Archiver to configure the settings for each mail server from which to archive. Additionally, you can set the polling frequency for all accounts, and temporarily disable journaling for these accounts from this page.
3. Upon saving, the Barracuda Message Archiver immediately begins pulling messages from the designated journaling accounts.

To include the journal envelope when exporting messages pulled from Microsoft Exchange journal accounts, go to **BASIC > Administration**. In the **Search Page Settings** section, turn on **Preserve Journal Wrappers**.

To set up a Designated SMTP Recipient:

1. Identify an email address that is to receive all journaled messages. This must be an account with the username **archiver** on your email server, and specified in the following format:
   `archiver@[`*`ip_address_of_Barracuda_Message_Archiver_inside_square_brackets`*`]`
   Example: `archiver@[192.168.2.24]`
2. Configure journaling on your email server so that all journaled messages are actually delivered to the designated email address.
3. If you created an account on your email server, then you must create a forwarding rule on your email server to deliver all messages received by that user to the Barracuda Message Archiver.

How to Archive Microsoft Non-Email Items

In addition to emails that are automatically sent from your Microsoft Exchange Server to the Barracuda Message Archiver for storage, you can also configure non-email items such as Appointments, Contacts, Notes, and Tasks for archive. This enables you to get a more complete picture of all items that are or have been stored on your Exchange server, and eliminates the need to keep .pst files around solely for the purposes of retaining this information.

The archiving, or synchronization, of all non-email items is configured on the **MAIL SOURCES > Exchange Integration** page. You can configure synchronization of all or a portion of the Outlook items, be it for all or selected users, on a recurring basis.

For details on archiving Microsoft Exchange Server 2007 or 2010 non-email items, refer to Microsoft Exchange Server 2007 and 2010 Deployment Template.

For details on archiving PST files, refer to the Barracuda PST Collector.

How to Synchronize Folders

This article refers to the Barracuda Message Archiver release 3.1 or higher.
In firmware release 3.5GA and higher, Folder Sync data automatically synchronizes between Barracuda Message Archivers in a High Availability cluster.

Synchronize Folders

The nightly folder synchronization process scans the specified Microsoft Exchange Server user mailboxes, and imports the user's folder structure, including custom folders and sub-folders, into the Barracuda Message Archiver. Note that a **Folder Sync** job does not import emails to the Barracuda Message Archiver, it only imports the folder structure. Email messages are sent to the Barracuda Message Archiver via real-time journaling or other supported means of mail transfer.

You can specify folder structure synchronization for all or selected users on the **MAIL SOURCES > Exchange Integration** page based on the selected item source, and optionally specify a specific server from which to archive. This synchronization process runs nightly.

Moving Email Between Folders

When the user moves an email between folders, the Barracuda Message Archiver updates the location of the email once the next nightly folder sync job runs and captures the new email location information. Additionally, the Barracuda Message Archiver keeps track of all folders in which an email has historically been located. Note that this does not cause any extra copies of the mail to be stored; the association is actually performed by associated the email message ID and the name of the folders in which the email should be shown.

The Message Archiver will keep track of all folders an email has historically been seen in. This does not cause any extra copies of the mail to be stored; the association is actually performed by associating the messageID of the email and the name of the folder(s) that the email should be shown in.

Understanding Which Folders are Synchronized

Outlook system folders (e.g., **Drafts**, **Sync Issues**), **Inbox**, **Deleted Items**, and **Sent Items** are not synchronized; a user's custom folders under **Inbox** are scanned. In the Barracuda Message Archiver's folder view, data is shown in **Inbox** and **Sent Items** based upon the header information in the mail itself. An email displays in a user's **Inbox** if that user is on the recipient list, and is visible in their **Sent Items** if the user's SMTP address, or email aliases, appears in the **From** header of the email.

If email is sent to the Barracuda Message Archiver via journaling, any emails in **Deleted Items** will have already been archived to the Barracuda Message Archiver from the **Inbox**.

How to Import GroupWise Messages

To archive messages from Novell® GroupWise® Servers to the Barracuda Message Archiver, each GroupWise server must have **Message Retention** enabled, and you must create a GroupWise Trusted Application Certificate.

Related Articles
• GroupWise Deployment • Understanding GroupWise Trusted Application Keys • How to Create a GroupWise Trusted Application Key

Additional Resource
• Barracuda Networks Knowledgebase Solution #00 002510

This article assumes you are downloading the **Trusted Application Key Generator** from the **USERS > Client Downloads** page to generate the GroupWise Trusted Key. To manually generate a key, see the article How to Create a GroupWise Trusted Application Key .

To enable archiving with Novell GroupWise:

1. Follow the instructions provided in your Novell GroupWise manual for enabling **Message Retention**. Directions are also provided on the Novell web site.
2. Log into a workstation that has the GroupWise client, the Novell 32-bit client installed, and is logged into the same eDirectory tree as the GroupWise server.
3. From that workstation, open a web browser and download the **Trusted Application Key Generator** from the **USERS > Client Downloads** page.
4. From that workstation, execute the downloaded Key Generator to create a Trusted Application Key to be uploaded onto the Barracuda Message Archiver; you must know the location of the domain directory.
5. Navigate to the **MAIL SOURCES > GroupWise Sync** page on the Barracuda Message Archiver.
6. Configure the items in the **GroupWise Synchronization** section for each GroupWise server. The generated Key should be entered in the **Trusted Application Key** field.
7. Save your changes to enable the Barracuda Message Archiver to maintain synchronicity with your GroupWise server.

Retention Time
For GroupWise retention time, the Barracuda Message Archiver sets the *digest* retention time; the *modified* retention time is not used or changed. However, GroupWise references the *modified* retention time to determine if a user is allowed to empty their trash. If a system administrator has manually set the *modified* retention time, or this value has been populated by a utility or application, the user may be unable to empty their trash until the *modified* retention time value is cleared for the mailbox.

For more information regarding Message Retention on your GroupWise server, refer to your Novell GroupWise documentation or the Novell website.

Understanding GroupWise Trusted Application Keys

Related Articles
• Importing Novell GroupWise Messages • How to Create a GroupWise Trusted Application Key

The Trusted Application Key was introduced in Novell® GroupWise® release 6.5 as a way of providing trusted third-party applications, such as the Barracuda Message Archiver, a method of logging into user mailboxes as a "super user" and allowing them to access the account without requiring the user password. The Trusted Application Key is generated through specialized APIs included with the third-party vendor software.

The Trusted Application Key provides access to every account in the GroupWise system. You can secure the Trusted Application Key from unauthorized use by specifying a retention flag against the Trusted Application Key. A retention flag allows the Barracuda Message Archiver to ensure 100% retention. See the Novell website for details on creating retention flags.

How to Create a GroupWise Trusted Application Key

This article refers to the Barracuda Message Archiver release 3.1 and higher, and Novell® GroupWise®.

In this article

- Naming the Trusted Application Key for the Barracuda Message Archiver
- Validating the Trusted Application
- Locating the Trusted Application Key

Related Articles

- Importing Novell GroupWise Messages
- Understanding GroupWise Trusted Application Keys

A Trusted Application Key is created at the Domain database level. To create this key, you need the following:

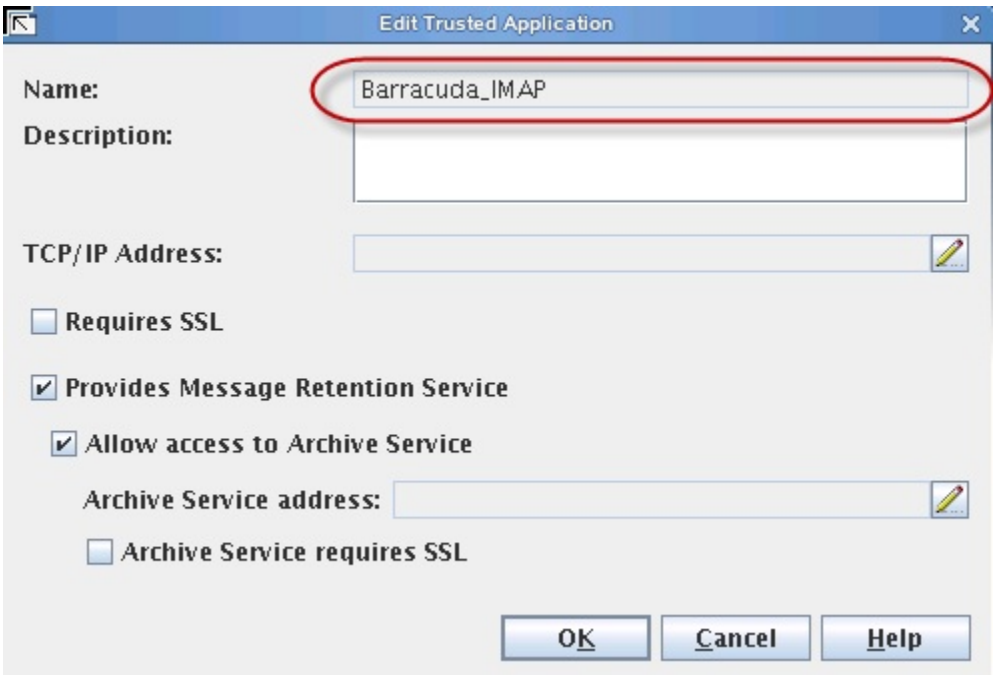
- An application capable of creating the Trusted Application Key such as the **GroupWise Trusted App Key Maker** available on the **USERS > Client Downloads** page of the Barracuda Message Archiver
- Administrator access to the GroupWise wpdomain.db database
- Administrator privileges to the Domain object within eDirectory

As with the majority of GroupWise administration, information is written to the Domain database, which is then propagated throughout the system. Information is replicated to other Domain databases which in turn push this information to the Post Office database. Therefore, it is critical when creating a Trusted Application Key that all Domains are communicating and show OPEN status in the Message Transfer Agents (MTAs).

Note that propagation of the Trusted Application Key to the Post Office database is based on the size of the GroupWise system; allow the Trusted Application Key to fully propagate before attempting to log in.

Naming the Trusted Application Key for the Barracuda Message Archiver

You must name the Trusted Application Key Barracuda_IMAP



Validating the Trusted Application

If the application is having difficulty running, or if the Trusted Application Key does not generate properly, review the Post Office Agent (POA) log files for the Post Office database you are trying to access using the Trusted Application Key. Locate the log entry for the login attempt: TRUSTED APP login attempt

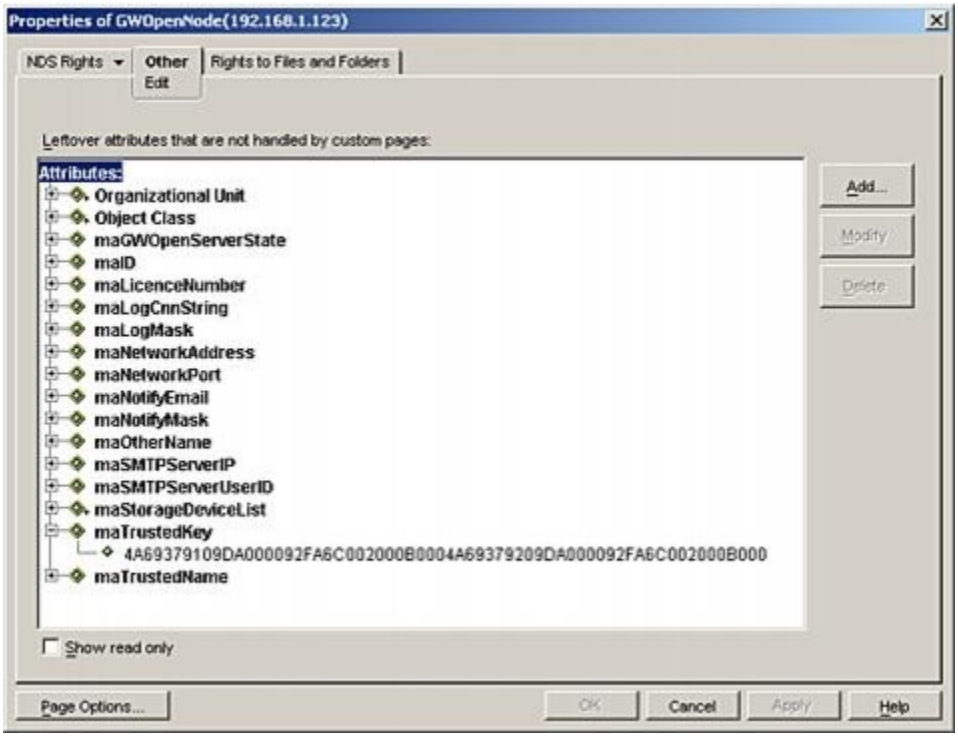
If the login attempt fails, there may have been issues encountered during the creation of the Trusted Application Key. Use the following steps to troubleshoot the Trusted Application Key:

1. Validate that the key lists the Trusted Application Key in eDirectory. The actual key is a 64-byte alpha-numeric string, for example:
   B346A421039D0000803225001F008000B346A422039D0000803225001F008000
   If the key does not look similar to this example, or if it contains non alpha-numeric characters, such as ¬, it is likely due to insufficient rights to the domain object in eDirectory when creating the object.
2. If the key structure is valid, it may be that the key credentials did not propagate to the Post Office database; perform a database rebuild on the Post Office database, and restart the POA.
3. The SINGLE-SIGNON setting on the Novell Client can also cause issues with the Trusted Application Key. If this property is activated, then the Trusted Application Key cannot log in to any account on the server unless the workstation is authenticated to eDirectory using that *same* account. If you can run the application when using the same GroupWise account as the account with which you are logged into eDirectory but you cannot access any other accounts, then run the GroupWise Client on the station and ensure that Single Sign-On is turned *off*.
4. If you are still unable to log in, delete the TRUSTED APP from ConsoleOne and regenerate using the GroupWise Trusted Application Key Maker available from the **USERS > Client Downloads** page in the Barracuda Message Archiver.

Locating the Trusted Application Key

If the Trusted Application Key is not properly regenerating in ConsoleOne, use the following steps to delete the Trusted Application Key from the eDirectory Configuration Container of the GroupWise POA:

1. To locate your Trusted Application Key, launch ConsoleOne, and then locate the **Group Wise Node** object.
2. Right-click on the **GW POA** object, and select **Properties**.
3. In the **Properties** dialog box, click the **Other** tab.
4. Under **Attributes**, expand the tree under **Trusted Application Key**:



How to Import IBM Notes NSF Files

This article refers to firmware version 3.5 or later and IBM® Notes®/IBM Domino® 8.5 or later running on a Microsoft Windows-based system.

In this article

- Import Options
- Barracuda Message Archiver NSF Import Utility
- NsfDump.exe Command

Related Articles
• IBM Notes/IBM Domino IMAP Deployment

Because the IBM Domino attachment and object service (DAOS) stores file attachments in a separate repository on the server that are retrieved by reference, before working with the NSF Import Utility, first restore these attachment objects to the customer mailbox.

Important
Barracuda Networks products interface with third-party products for email archival. Barracuda is not responsible for the performance or functionality of third-party products.

In some instances, Lotus Notes NSF imports have caused corruption of the data. The source of the corruption appears to be the third-party software. As a result, we recommend that you back up your data *before* importing an NSF file through the NSF Importer tool.

Import Options

Message Import
When using the NSF Import Utility or NsfDump.exe command, there is a 2048MB limit on file import.

You can import a single NSF file using the NSF Import Utility, or use the **NsfDump.exe** file for batch file automation.

On the system running IBM Notes, copy all of the NSF files you wish to import to a single directory.

Barracuda Message Archiver NSF Import Utility

Use the following steps to import a single NSF file using the Barracuda Message Archiver NSF Import Utility:

1. Log into the Barracuda Message Archiver web interface, and go to the **USERS > Client Downloads** page.
2. In the **Lotus Notes** section, download and install the **NSF Import Utility** on a Microsoft Windows-based system on which IBM Notes is installed.
3. From the **Start** menu, launch the **Barracuda Message Archiver NSF Import Utility**, and follow the instructions to import an NSF file.

NsfDump.exe Command

Use the following steps to automate the import of multiple IBM Notes NSF files:

1. Log into the Barracuda Message Archiver web interface, and go to the **USERS > Client Downloads** page.
2. In the **Lotus Notes** section, download and install the **NSF Import Utility** to a Microsoft Windows-based system on which IBM Notes is installed.
3. From a command prompt, run the **NsfDump.exe** command using your directory and Barracuda Message Archiver parameters; note that **`Http`** represents your Barracuda Message Archiver *hostname*, not a URI or port:
   ```
   NsfDump.exe -NsfDirectory "C:\NsfFiles" -JobDirectory "C:\NsfDump" -Http "archiver.example.com"
   ```

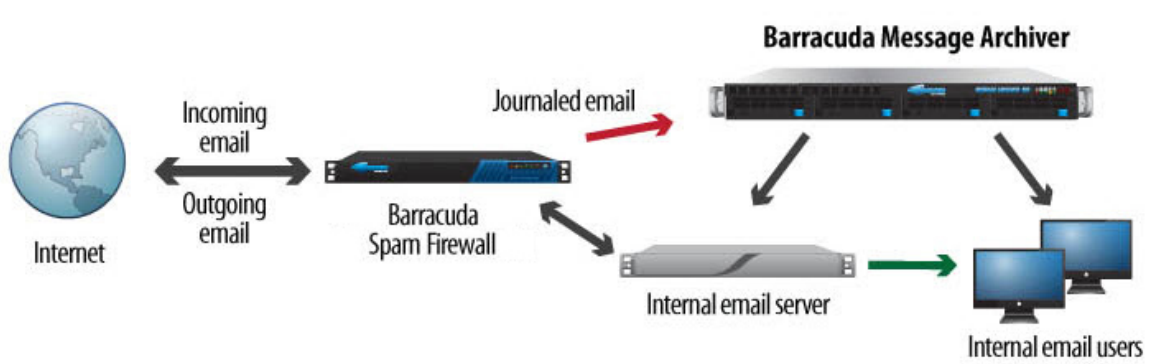
Note that NsfDump.exe also supports the `-Nsf` command to import single NSF files if `NsfDirectory` is not suitable for some reason. This allows you to automate import using the desired approach, for example batch files.

How to Configure Your Barracuda Message Archiver to Act as an SMTP Proxy to Your Email Server

Related Articles
• Understanding Email Encryption and Archival • How to Set Up Email Encryption and Archival

If you have a Barracuda Spam Firewall, and your email server has journaling capabilities, it is recommended that you set up Remote Journal Accounts as outlined in How to Set Up Email Journaling. However, if your email server is *not* able to journal messages, you can configure your Barracuda Message Archiver to act as an SMTP proxy to your email server and activate the journaling feature that is available on the Barracuda Spam Firewall to submit messages to the Barracuda Message Archiver.

Important
The Barracuda Message Archiver MUST be configured to be the SMTP relay even for all internal email traffic because messages that bypass the Barracuda Spam Firewall are not available for journaling. The following image illustrates the required traffic flow:



To set up journaling on your Barracuda Spam Firewall:

1. Navigate to the **BASIC > Administration** page, and look in the **Mail Journaling** section.
2. In the **Destination Email Address** field, enter an SMTP recipient in the form:
   `archiver@[ip_address_of_Barracuda_Message_Archiver]`
   Example: `archiver@[192.168.2.24]`
3. In the **Bounce Address** field, enter the email address that is to receive all bounce notifications from the Barracuda Message Archiver.
4. Click **Save Changes**.
5. The Barracuda Spam Firewall begins sending a copy of every delivered message to the Barracuda Message Archiver. You must configure the **ADVANCED > SMTP Proxy** setting on the Barracuda Message Archiver to forward messages to your email server.

How to Import Historical Data

This article refers to the Barracuda Message Archiver release 3.1 or higher.

In order to get the most complete archive possible, the Barracuda Message Archiver archives not only new messages, but also any existing (stored) items that were either already on your email server or stored in **.pst** files.

In this article

- Direct Imports (via MAPI)
- PST File Imports
  - Immediate Import
  - Queued Imports
- Upload Share Settings

Related Articles

- Barracuda PST Collector
- How to Assign and Unassign PST Files

Stubbing and Microsoft Exchange Import
For stubbing and Microsoft® Exchange imports initiated via the Barracuda Message Archiver web interface, there is a 100MB limit on file import.

Direct Imports (via MAPI)

All emails currently on your Microsoft Exchange Server can be imported directly into the Barracuda Message Archiver via Microsoft's Message Application Protocol Interface (MAPI).

You can configure multiple Exchange servers on the **MAIL SOURCES > Exchange Integration** page to import to the Barracuda Message Archiver. A list of all imports currently in progress, as well as those most recently completed, are available along with details for each import, including real-time monitoring of imports in progress.

For details on using the Exchange Integration feature, refer to the following articles:

- Firmware release 3.2 and earlier - Microsoft Exchange Server 2003, 2007, and 2010 Integration
- Firmware release 3.5 or higher - Microsoft Exchange Server Integration

PST File Imports

A **.pst** file is an MS Personal Storage Table, and contains email messages exported from Microsoft Outlook. Some **.pst** files also contain additional Microsoft Outlook items such as Appointments and Contacts. You can import the contents of any **.pst** file from Microsoft Outlook 2000 (and later) into the Barracuda Message Archiver from the **MAIL SOURCES > PST Import** page. Password-protected **.pst** files are accepted as well as non-password-protected files.

> **Important**
> Before importing .**pst** files, ensure that LDAP services for your Active Directory server are configured on the Barracuda Message Archiver from the **USERS > Directory Services** page. This ensures that SMTP aliases associated with the message sender and recipients are resolvable.

There are two methods to import a **.pst** file:

- **Immediate import** from the web interface (for single, small .**pst** files less than 250MB)
- **Queued import** (for multiple and/or large .**pst** files)

Immediate Import

The Barracuda Message Archiver can accept one .**pst** file at a time for immediate import from the web interface. Files that are imported directly in this manner are processed immediately and their contents added to the Barracuda Message Archiver. Because processing files for import can be resource-intensive, Immediate Import supports files of less than 250 MB in size. If you have any large files, or if you have multiple smaller files to import, use the Queued Import method described below.

Queued Imports

Queued importing separates out the uploading step of importing a .**pst** file from the actual processing step. This is highly recommended if you have multiple .**pst** files whose contents you wish to add to the archive, allowing you to easily place .**pst** files on the Barracuda Message Archiver, and to delay file processing until a time when system performance is least impacted. Use Queued Import for large **.pst** files (greater than 250 MB) as this allows you to upload files "in the background," thus reducing the risk of file transfer interruptions and browser timeouts.

Uploaded files are placed on a resident share on the Barracuda Message Archiver, and are listed on the **MAIL SOURCES > PST Import** page. Any uploaded files must then be imported in a separate step. You can choose to initiate multiple file processing in a single step, or select to process one file at a time. Any passwords required to access the contents of the .**pst** file must be specified here prior to initiating the import process.

> **Important**
> All **.pst** files of greater than 2 gigabytes can only be added to the Barracuda Message Archiver via Queued Import.

Upload Share Settings

By default, only the administrator's web interface has access to view the files currently on the share, to upload files onto the share, and to initiate processing of any files on the share. You can choose to provide access to the upload area to other users as an SMB/CIFS share (with an optional Workgroup name and password), to make it easier to copy/paste or drag/drop any .**pst** file for import. When enabled, the share is accessible in the following manner:

`\\IP\BarracudaMessageArchiverPstDrop`

For example, if your Barracuda Message Archiver has the IP address of 192.168.2.24, use the following to connect to the share:

```
\\192.168.2.24\BarracudaMessageArchiverPstDrop
```

To allow access to the share to upload a .**pst** into the Barracuda Message Archiver, the administrator must enable and configure the **PST Import Options** from the **BASIC > Administration** page. Privileges can be assigned to all users, or to just a single password-protected account called **pstdrop** to be used by anyone with the password.

Microsoft Exchange Server Integration

This article refers to the Barracuda Message Archiver release 3.5 and higher, and Microsoft® Exchange Server 2003, 2007, 2010, and 2013.

If you are using firmware version 3.2 and earlier, refer to the article Microsoft Exchange Server 2003, 2007, and 2010 Integration.

In this article:

- Exchange Integration
- Select Action
- Select Server
- Configure Action
- View Summary

Related Articles

- How to Enable RPC over HTTP Connectivity

Additional Resources

- For detailed information, go to the **MAIL SOURCES > Exchange Integration** page, and click **Help**.

The Exchange Server Import feature does not work with disabled user accounts. To import content from disabled accounts, you must temporarily enable the accounts in Exchange. If users are hidden from the Global Address List (GAL) in Exchange, their emails cannot be imported; you must temporarily unhide these accounts to import their email.

Exchange Integration

Use the **New Action** Workflow in the **MAIL SOURCES > Exchange Integration** page to configure all actions that the Barracuda Message Archiver is to execute on your Microsoft Exchange Server.

Only one operation can run at any given time, so operations submitted while one is already in progress are placed in a queue for execution in the order submitted as soon as previous operations complete. All submitted operations are added to the **Recent Actions** table, with the most recent ones at the top.

Select Action

Select the type of action to perform on the Exchange Server:

- **Email Import** – Import all email from your Exchange Server into the Barracuda Message Archiver that meets the specified criteria. Select to import email for all users, or specify import by user name, email address, last name, public folders, or a distribution list.
- **Non-Email Sync** – Import only non-email Exchange items into the Barracuda Message Archiver from specified accounts including Appointments, Contacts, Tasks, and Notes.
- **Email Stubbing** – Locate messages on your Exchange Server that meet the specified criteria, copy the specified parts (just attachments, or the entire message with or without attachments) onto the Barracuda Message Archiver, and modify those messages on your Exchange Server so that appropriate parts of the messages are replaced with a stub (a link to where the actual contents reside on the

Barracuda Message Archiver).

- **Folder Sync** – Import into the Barracuda Message Archiver the complete folder structure of the selected users' Mailboxes. This action imports the selected users' custom folders and subfolders.

Select Server

Select an existing Exchange Server, copy an existing Exchange Server configuration to modify, or add a new Exchange Server configuration. To enable RPC over HTTP (RoH), refer to the article How to Enable RPC over HTTP Connectivity.

Configure Action

Use this page to configure settings for the selected action using the Workflow fields.

View Summary

The View Summary page in the Workflow displays the Exchange Server action details. From this page you can click **Simulate Action** to perform a "dry run" of the selected action on the Exchange Server, by looking for and identifying the items meeting the specified criteria without actually executing any action on those messages. All items that meet the specified criteria are listed in the Activity Log for that operation, but no actual content on the Exchange Server is modified. Note that once you click **Simulate Action**, an entry is added to the **Recent Actions** table. Click the **Report** link in the **Recent Actions** table to review the results for the operation.

> **Email Stubbing**
> If you simulate an Email Stubbing process, make sure to reset the Schedule to Nightly if you want this to run nightly as opposed to immediately.

Click **Submit** to add the action to the **Scheduled Actions** table and close the workflow.

Microsoft Exchange Server 2003, 2007, and 2010 Integration

> This article refers to the Barracuda Message Archiver release 3.2 and earlier, and Microsoft® Exchange Server 2003, 2007, and 2010.
>
> If you are using firmware version 3.5 and higher, refer to the article Microsoft Exchange Server Integration.

In this article:

- Exchange Integration
- Recent Actions

Use the steps in this article to automatically import, stub, and synchronize Microsoft Exchange Server folder data that is to be archived on the Barracuda Message Archiver.

> The Exchange Server Import feature does not work with disabled user accounts. To import content from disabled accounts, you must temporarily enable the accounts in Exchange. If users are hidden from the Global Address List (GAL) in Exchange, their emails cannot be imported; you must temporarily unhide these accounts to import their email.

Exchange Integration

Use the following steps to set up Exchange Server integration:

1. Log into the Barracuda Message Archiver web interface, and go to the **MAIL SOURCES > Exchange Integration** page.
2. Enter the Exchange Server details in the **Exchange Integration** section:
   - **Exchange Server** - Enter the Exchange Server hostname or FQDN; this value must be resolvable by your configured DNS servers to the correct IP address.
   - **Username/Password** - Enter an authorized Exchange Server account username and password

     > You must have an Exchange Server account with permissions to access the entered username. Additionally, this account must meet the following requirements:

- Has a mailbox;
- Visible on the GAL;
- Read-As, Write-As, and Administer-Store access to the target mailboxes;
- Account must not be locked.

An Exchange Server Administrator account does not necessarily meet these requirements.

For more information, refer to the following articles:

- Creating an Email Service Account for Microsoft Exchange Server 2003
- Creating an Email Service Account for Microsoft Exchange Server 2007, 2010, and 2013

The password should be alphanumeric; a timeout can occur if characters such as **!@#$%^&*()** are included in the password.

- **Domain** - Enter the domain for the authorized account specified in the **Username** field.

- The Exchange domain may not be the same as your DNS domain.
- If the Barracuda Message Archiver cannot resolve the specified domain, go to the **BASIC > IP Configuration** page and specify the DNS server to one of your Windows domain controllers.

3. Specify the desired import, synchronization, and stubbing action settings based on the details in **Table 1** below (for additional details, click the **Help** button on the **MAIL SOURCES > Exchange Integration** page in the web interface).
4. Once you set up your import, synchronization, and stubbing details, click on one of the following buttons:
   a. **Scheduled Action** - Click to start the specified actions on the Exchange Server.
   b. **Simulate Action** - Click to perform a dry run of the selected actions on the Exchange Server. This allows you to review your settings before actually importing content.
   c. **Verify Sources** - Click to view a list of the individual mailboxes that are to be used based on the provided parameters.

Table 1. Action Settings by Tab.

Tab/Section		Description
Email Import		Imports all items matching the item source filter from the specified Exchange Server into the Barracuda Message Archiver for processing.
	Item Date	Only items matching this date restriction are imported.

	Item Source	Select the target list from which to import:
		• **Public Folders** - Looks in all public folders on the specified Exchange Server.
		• **Distribution List** - Looks for items that are sent to the individual accounts that receive content sent to the list entered in the associated field.
		• **Users** - Looks for items sent to specified users:
		  • **All Users** - All users on the specified Exchange Server
		  • **Last Name** - Any user on the specified Exchange Server whose last name matches the value entered in the associated field.
		  • **Email Address** - Any email account that matches the value entered in the associated field. Enter an entire email address (including the domain name) or only a portion to match multiple addresses.
		• **Folders** *(Users only)* - If you select the **Item Source** as **Users**, you can specify from which folders to pull messages.

	Advanced Settings	• **Home Server** - Enter the hostname or IP address of the server housing the message store to search through. • **Maximum Size (KB)** - Enter the maximum acceptable size for a message to be inspected. Messages larger than the entered size are bypassed.
Synchronize Non- Email Items		This is a one-time task to import non-email items.
	Item Type	Select the type of data to import.

	Item Source	Select the target list from which to import:
		• **Public Folders** - Looks in all public folders on the specified Exchange Server.
		• **Distribution List** - Looks for items that are sent to the individual accounts that receive content sent to the list entered in the associated field.
		• **Users** - Looks for items sent to specified users:
		  • **All Users** - All users on the specified Exchange Server
		  • **Last Name** - Any user on the specified Exchange Server whose last name matches the value entered in the associated field.
		  • **Email Address** - Any email account that matches the value entered in the associated field. Enter an entire email address (including the domain name) or only a portion to match multiple addresses.
		• **Folders** *(Users only)* - If you select the **Item Source** as **Users**, you can specify from which folders to pull content.

	Advanced Settings	• **Home Server** - Restrict the action to only items residing on the configured server. • **Maximum Size (KB)** - Enter the maximum acceptable size for an item to be inspected. Items larger than the entered size are bypassed.
Email Stubbing		Imports messages that have attachments, and replaces either the message or the attachment with stubs and stores attachments on the Barracuda Message Archiver rather than on the mail server itself.
	Schedule	Designate whether to start stubbing immediately or nightly.
	Stub Content	Specify whether to stub only attachments or the entire message.
	Item Age (Days)	Only items that are the entered age or older are stubbed.
	Minimum Size (KB)	Items smaller than the entered value are not stubbed.

	Item Source	Select the target list from which to stub:
		• **Distribution List** - Looks for items that are sent to the individual accounts that receive content sent to the list entered in the associated field.
		• **Users** - Looks for items sent to specified users:
		  • **All Users** - All users on the specified Exchange Server
		  • **Last Name** - Any user on the specified Exchange Server whose last name matches the value entered in the associated field.
		  • **Email Address** - Any email account that matches the value entered in the associated field. Enter an entire email address (including the domain name) or only a portion to match multiple addresses.
		• **Folders** *(Users only)* - If you select the **Item Source** as **Users**, you can specify from which folders to pull content.

	Advanced Settings	• **Home Server** - Restrict the action to only items residing on the configured server. • **Maximum Size (KB)** - Enter the maximum acceptable size for an item to be inspected. Items larger than the entered size are bypassed.
Synchronize Folders		Synchronize folder structure from the Exchange Server mailboxes to the Barracuda Message Archiver for searching purposes. **Important:** This synchronization assigns emails that the Barracuda Message Archiver has already imported via other means to the folders they inhabit within a user's mailbox at the time the folder synchronization runs. No new emails are brought into the Barracuda Message Archiver by this job type.

	Item Source	Select the target list to synchronize:
		• **Distribution List** - Looks for items that are sent to the individual accounts that receive content sent to the list entered in the associated field.
		• **Users** - Looks for items sent to specified users:
		  • **All Users** - All users on the specified Exchange Server
		  • **Last Name** - Any user on the specified Exchange Server whose last name matches the value entered in the associated field.
		  • **Email Address** - Any email account that matches the value entered in the associated field. Enter an entire email address (including the domain name) or only a portion to match multiple addresses.
		• **Folders** *(Users only)* - If you select the **Item Source** as **Users**, you can specify from which folders to stub content.

	Advanced Settings	• **Home Server** - Restrict the action to only items residing on the configured server. • **Run Now** - Turn *On* to immediately synchronize the folders and schedule the job.

Schedule Actions

The **Scheduled Actions** table displays a list of operations that are currently in a queue awaiting execution. Click **Update** to update the table data.

Recent Actions

The **Recent Actions** table displays a list of operations that recently ran. Click **Update** to update the table data.

Understanding SMTP Forwarding and Trusted Servers

In this article:

- SMTP Forwarding
- Trusted SMTP Servers

Related Articles

- Configuring Envelope Journaling for Exchange 2013 - Standard Journaling
- Configuring Envelope Journaling for Exchange 2013 - Premium Journaling
- Configuring Envelope Journaling for Exchange 2007 and 2010
- Configuring an SMTP Journal Account for Exchange 2003

SMTP Forwarding

You can enable SMTP forwarding as a method for adding messages to the Barracuda Message Archiver, and also specify trusted hosts so that the Barracuda Message Archiver accepts only those messages forwarded by trusted (whitelisted) hosts. You enable SMTP forwarding on the **MAIL SOURCES > SMTP/IM** page. When enabled, and one or more IP addresses are listed as trusted, mail is accepted only from the listed IP address; mail is blocked and not archived if the source is from an IP address not listed in this section. When disabled, and one or more IP addresses are listed as trusted, mail coming from a listed IP address is accepted no matter the domain present in the SMTP envelope of the inbound mail, and mail coming from an IP address not listed in this section is rejected if the SMTP envelope does not contain a domain listed in the **Local Domains** section on the **BASIC > IP Configuration** page.

Trusted SMTP Servers

Trusted forwarding servers are those servers whose messages are to be accepted and archived by the Barracuda Message Archiver. When SMTP forwarding is enabled on the **MAIL SOURCES > SMTP/IM** page, add the IP addresses of all trusted forwarding servers that will send messages to be archived in the **Trusted SMTP Servers** section of the page. All messages arriving from the servers listed here are always added to the archive regardless of the domain name present in the SMTP envelope. Any messages forwarded from servers *not* in this list are rejected.

If you are using Microsoft Exchange and are using Envelope Journaling to send messages to the Barracuda Message Archiver via SMTP, add the IP address of each Exchange Server to this section.

If no IP addresses are listed in this section, the Barracuda Message Archiver accepts email for domains listed in the **Local Domains** section on the **BASIC > IP Configuration** page if that domain is present in the SMTP envelope of the inbound email.

Exchange Stubbing

This article refers to the Barracuda Message Archiver release 3.1 and higher, and Microsoft® Exchange Server.

in this article

- Frequency
- Policy-Based Stubbing
- End-User Controls
- Unstubbing
- Restoring Stubbed Content to Microsoft Exchange

Related Articles

- Installing & Configuring the Outlook Add-In
- Mobile Application for iPhone, iPod Touch, and iPad
- Mobile Application for Android
- Retrieving Stubbed Messages in Shared Mailboxes

Stubbing and Microsoft Exchange Import
For stubbing and Microsoft Exchange imports initiated via the Barracuda Message Archiver user interface, there is a 100MB limit on file import.

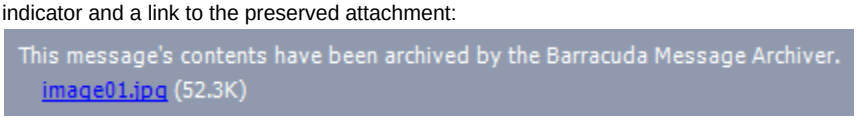
Whitespace Recovery
Once stubbing is complete, view the Microsoft technet article Eseutil /D Defragmentation Mode to determine how best to recover whitespace located within the Exchange Server mailstore.

Some administrators of Microsoft Exchange servers may wish to enable stubbing to store attachments on the Barracuda Message Archiver rather than on the mail server itself, since doing so can greatly increase the storage capacity of their mail server, in some cases by as much as 70%.

Exchange Stubbing configuration is done on the **MAIL SOURCES > Exchange Integration** page.

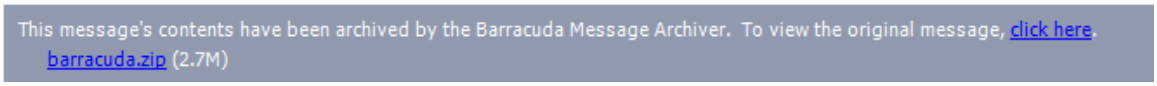
During the stubbing process, the Barracuda Message Archiver adds all attachments (**Attachments Only** option), or the entire message (**Entire Message** option) for a message to its own storage database and creates a hyperlink, or stub, to the original attachment or message depending on the option you select in the **Exchange Integration** page. The attachment from the original message, or if selected, the entire message, is then removed from your Exchange server and replaced with the stubs so that any requests to access the file or message is automatically redirected to, and served from, the Barracuda Message Archiver. A short message containing the names and sizes of the stubbed content is placed in every "stubbed" email, along with a hyperlink from which users can easily access the attachments regardless of what email client is used, including Outlook Web Access and mobile devices.

- **Attachments Only** - When selected, the attachment is removed from the message and the attachment is replaced with an attachment indicator and a link to the preserved attachment:

If there are no attachments in the message, then nothing is stubbed and the entire message is left intact.

- **Entire Message** - When selected, the entire message body is replaced with a text excerpt containing a link to the original message:

  
  This message's contents have been archived by the Barracuda Message Archiver. To view the original message, click here.
barracuda.zip (2.7M)

Users of Microsoft Outlook 2003 and higher can view a stubbed email using the Barracuda Message Archiver Outlook Add-in. When a stubbed email is accessed through the add-in, the attachment is automatically downloaded and displayed as part of the original email. The attachment is readily available for viewing or dragging onto the desktop, making the stubbing process virtually invisible.

Important
In order for remote users of the Barracuda Message Archiver Outlook Add-in to interact with the Barracuda Message Archiver, the Web Interface Ports specified on the **BASIC > Administration** page and on the **ADVANCED > Secure Administration** page must be configured on your corporate firewall to accept incoming connections.

Frequency

The stubbing process can be initiated on demand or configured to run nightly. All messages that are currently on your Exchange Server that meet the provided criteria are stubbed. When configured to run nightly, the process starts between 2am and 3am when the additional system load on the Barracuda Message Archiver least impacts users.

Policy-Based Stubbing

The Barracuda Message Archiver only stubs messages that meet your specified criteria, which can be any combination of the following:

- **Mailbox** - Messages in the specified accounts
- **Age** - Messages older than the specified number of days
- **Size** - Messages larger than the specified size

You can configure multiple stubbing policies, including all stubbing procedures and their results and statuses, listed on the **MAIL SOURCES > Exchange Integration** page in the **Recent Actions** section.

End-User Controls

The Barracuda Message Archiver Outlook add-in is available to all users of Microsoft Outlook 2003 and higher, and retrieves the attachment and places it inline to ensure that email messages and attachments appear as they would prior to Exchange stubbing. The add-in can also be used to temporarily unstub and re-stub specific messages. Any message unstubbed via the add-in remains so for 30 days, after which time it is re-stubbed during the next automatic stubbing process.

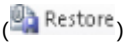
Unstubbing

Unstubbing a message causes the Barracuda Message Archiver to place the attachment back into the body of the message. This is most useful when individual end-users are on the road and need immediate access to all attachments in a message even while not directly connected to the mail server. Any message that is unstubbed by the user remains so until it is re-stubbed by that user, or after 30 days; it is not re-stubbed by

either an immediate or nightly stubbing process during this time.

Restoring Stubbed Content to Microsoft Exchange

> **Firmware Version**
> This feature is available only in the Barracuda message Archiver Outlook Add-In version 3.2.30 and higher.

To restore stubbed content to your Microsoft Exchange Server, click the **Restore** (

) icon in the Outlook toolbar. When clicked, the selected stub content is restored to the Exchange Server and persists on the Server for 30 days.

How to Retrieve Stubbed Messages in Shared Mailboxes

This article refers to the Barracuda Message Archiver release 3.1 or higher, and the Barracuda Message Archiver Outlook Add-In version 3.1 or higher, and Microsoft ® Outlook ® 2003, 2007, or 2010.

In this Article :

- Enable Scripting Organization-Wide (Recommended)
- Enable Scripts on User Systems
  - Enable Scripts in Microsoft Outlook 2003
  - Enable Scripts in Microsoft Outlook 2007
  - Enable Scripts in Microsoft Outlook 2010

Related Articles

- Barracuda Message Archiver Outlook Add-In Deployment

> **Configuration Guidelines**
> This article is intended as a configuration *guideline*; your deployment will be specific to your environment. Any administrative changes should be reviewed with your IT team before proceeding.

Use the steps described in this article if Outlook users are able to forward stubbed attachments or emails from their *own* Outlook mailbox, but not from a *shared* Outlook mailbox. If this is the case, users will receive an error message from Outlook similar to: "**Unable to open original message**" when attempting to forward stubbed attachments from a shared Outlook mailbox.

By default in Microsoft Outlook 2003, 2007, and 2010, a security setting does not allow script execution or custom forms in shared mailboxes or public folders. For this reason, if the Microsoft Exchange Administrator performs message stubbing on shared mailboxes or public folders delegated to all users or specific user groups, these stubbed messages cannot be retrieved in the Barracuda Message Archiver Outlook Add-In. To allow users to retrieve these stubbed messages in addition to their **INBOX** messages, each user can set **Allow Script in shared folders**, or the Microsoft Exchange Administrator can enable scripts in folders organization-wide using the Microsoft Office policy template (ADM) files.

> **Microsoft Outlook 2013**
> In Microsoft Outlook 2013, script execution is allowed by default.

Enable Scripting Organization-Wide (Recommended)

To enable scripts across your entire organization, go to the associated Microsoft article:

- Microsoft Outlook 2003 - See the Microsoft article Office 2003 Service Pack 3 Administrative Template (ADM) OPAs, and Explain Text

Update, verify your operating system in the section ***System requirements***, and following the steps described in the section ***Instructions***.

- Microsoft Outlook 2007 - See the Microsoft article 2007 Office system Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool version 2.0, your operating system in the section ***System requirements***, and following the steps described in the section ***Instructions***.
- Microsoft Outlook 2003 - See the Microsoft article Office 2010 Administrative Template files (ADM, ADMX/ADML) and Office Customization Tool download, verify your operating system in the section ***System requirements***, and following the steps described in the section ***Instructions***.

Once you download and set up the ADM template files, open the associated Outlook ADM file:

- For Outlook 2003, open the ADM file **outlk11.adm**
- For Outlook 2007, open the ADM file **outlk12.adm**
- For Outlook 2010, open the ADM file **outlk14.adm**

In the ADM file, set `VALUEON NUMERIC` to '`1`' and `VALUEOFF NUMERIC` to '`0`' for the following values:

- `VALUENAME SharedFolderScript`
- `VALUENAME PublicFolderScript`

For example, update the ADM file **outlk11.adm** to display as:

```
POLICY "Disable scripts for shared folders"

KEYNAME Software\Policies\Microsoft\Office\11.0\Outlook\Security
        PART "Check to disable scripts for shared folders" CHECKBOX
                                VALUENAME SharedFolderScript
                                VALUEON NUMERIC 1 DEFCHECKED
                                VALUEOFF NUMERIC 0
        END PART
        END POLICY
POLICY "Disable scripts for public folders"
KEYNAME Software\Policies\Microsoft\Office\11.0\Outlook\Security
        PART "Check to disable scripts for public folders" CHECKBOX
                                VALUENAME PublicFolderScript
                                VALUEON NUMERIC 1
                                VALUEOFF NUMERIC 0
        END PART
        END POLICY
```

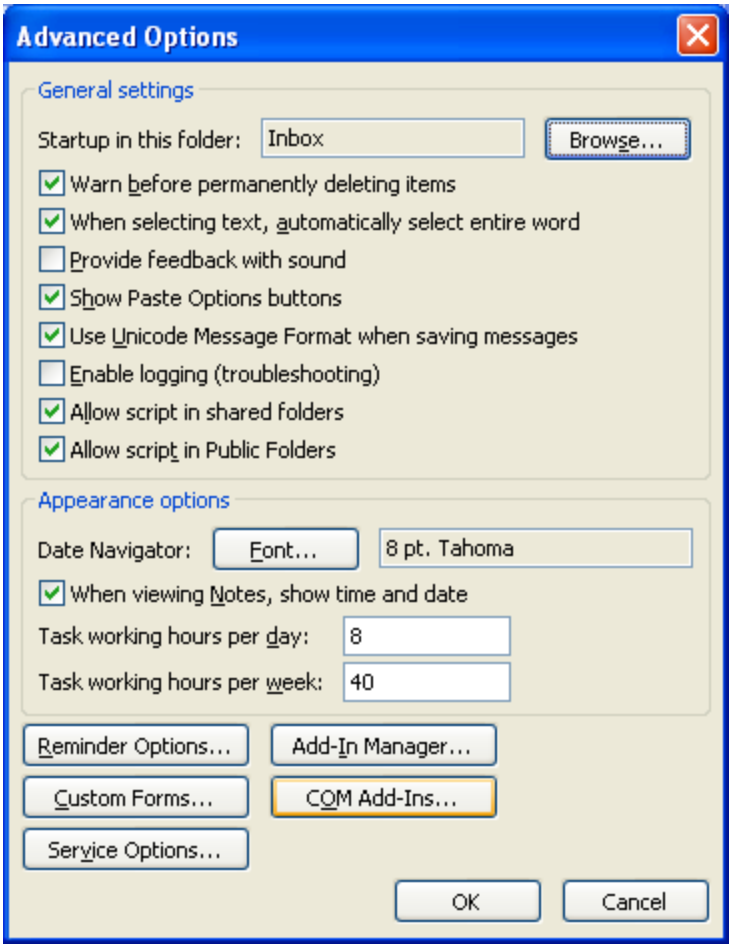
Enable Scripts on User Systems

If you do not wish to use ADM templates to allow scripting across the entire organization, you can direct each user to enable scripts for shared and public folders based on their installed version of Microsoft Outlook.

Enable Scripts in Microsoft Outlook 2003

Use the following steps to enable scripts in shared and public folders in Outlook 2003:

1. Log into Microsoft Outlook 2003.
2. On the **Tools** menu, click **Options**.
3. In the **Options** dialog box, click the **Other** tab, and click **Advanced Options**.
4. In the **General Settings** pane, select **Allow Script in shared folders** and **Allow script in Public Folders**:

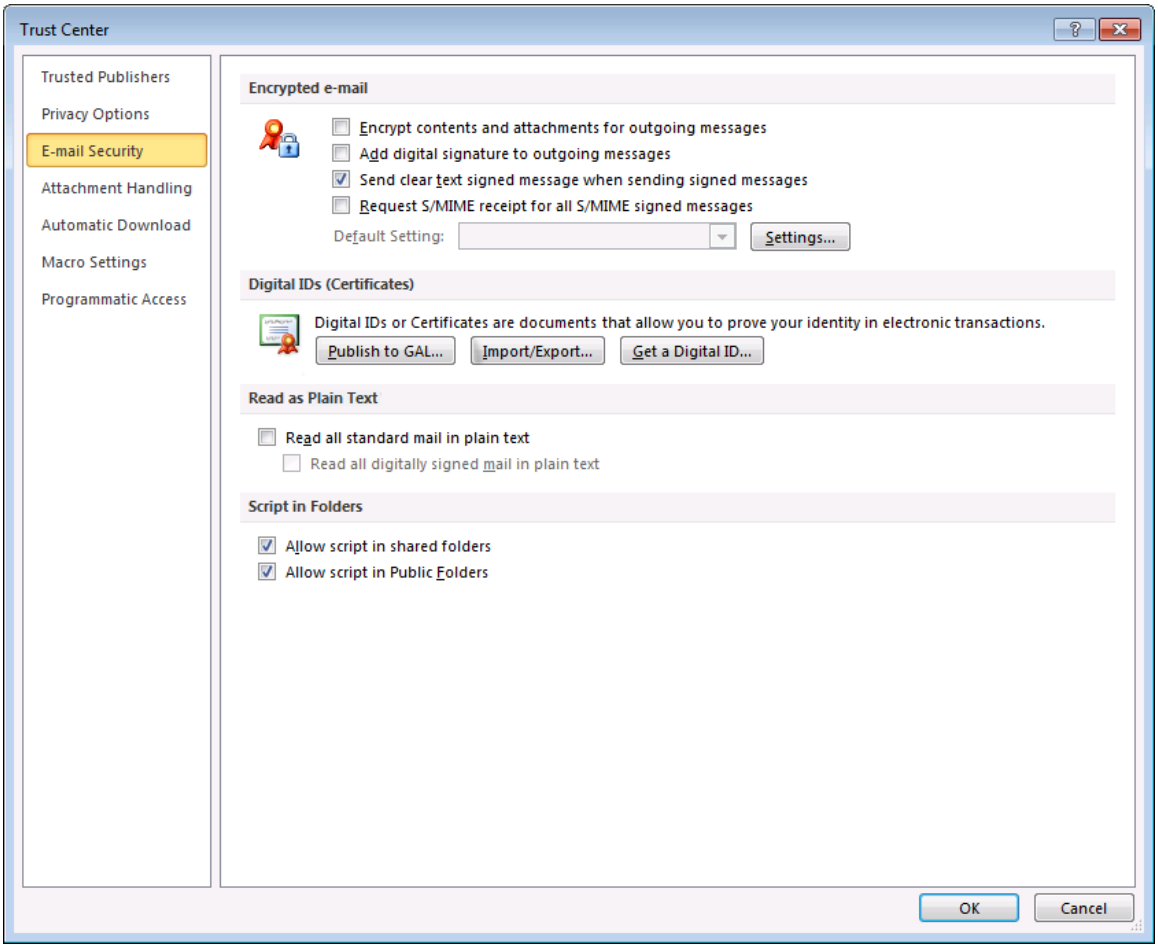


5. Click **OK** to save your settings.

Enable Scripts in Microsoft Outlook 2007

Use the following steps to enable scripts in shared and public folders in Outlook 2007:

1. Log in to Microsoft Outlook 2007.
2. On the **Tools** menu, click **Trust Center**.
3. In the Navigation Pane, click **E-mail Security**.
4. In the **Script in Folders** section, select **Allow script in shared folders** and **Allow script in Public Folders**:

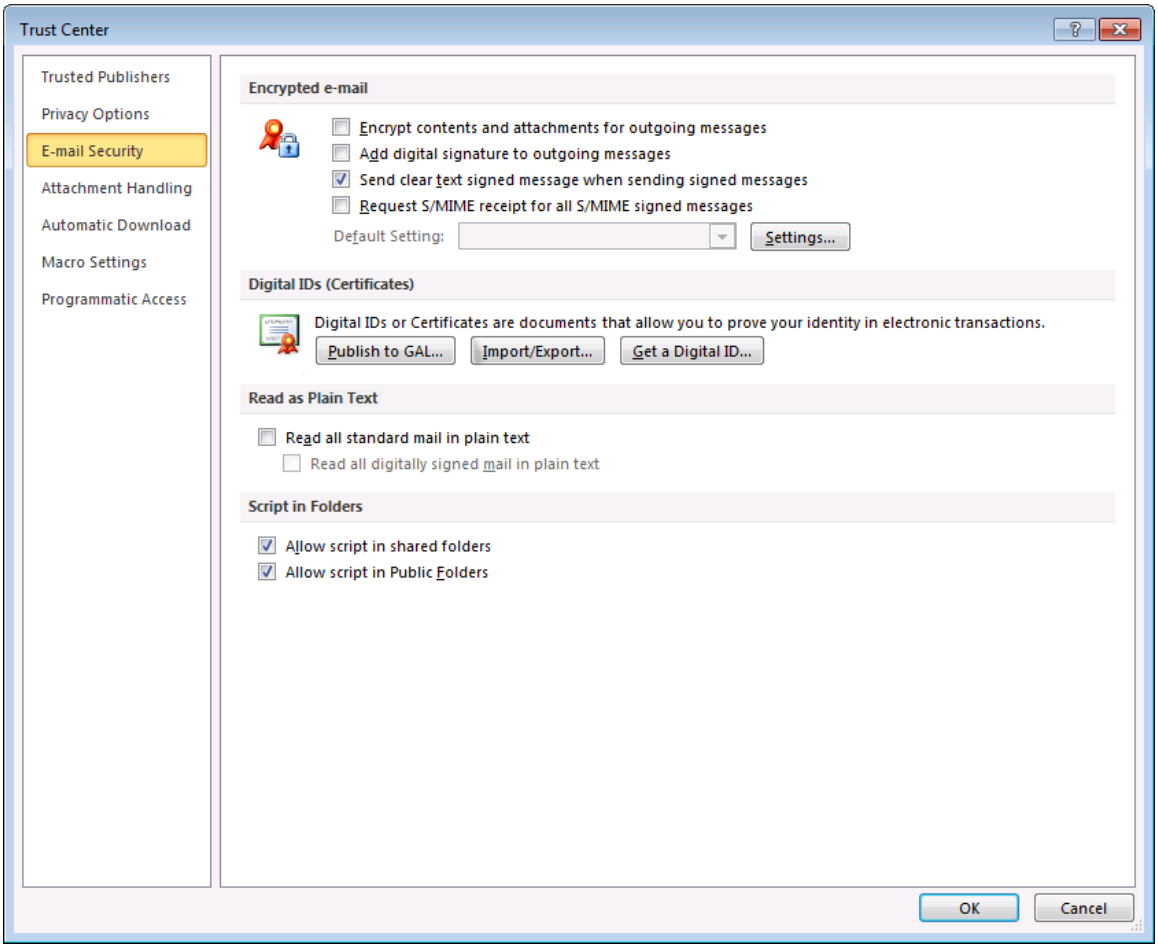

Trust Center
Trusted Publishers
Privacy Options
E-mail Security
Attachment Handling
Automatic Download
Macro Settings
Programmatic Access
Encrypted e-mail
Encrypt contents and attachments for outgoing messages
Add digital signature to outgoing messages
Send clear text signed message when sending signed messages
Request S/MIME receipt for all S/MIME signed messages
Default Setting:
Settings...
Digital IDs (Certificates)
Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.
Publish to GAL...
Import/Export...
Get a Digital ID...
Read as Plain Text
Read all standard mail in plain text
Read all digitally signed mail in plain text
Script in Folders
Allow script in shared folders
Allow script in Public Folders
OK
Cancel

5. Click **OK** to save your settings.

Enable Scripts in Microsoft Outlook 2010

Use the following steps to enable scripts in shared and public folders in Outlook 2010:

1. Log in to Microsoft Outlook 2010.
2. On the **File** menu, click **Options**.
3. In the Navigation Pane, click **Trust Center**, and then click **Trust Center Settings**.
4. In the Navigation Pane, click **E-mail Security**, and in the **Script in Folders** section, select **Allow script in shared folders** and **Allow script in Public Folders**:


Trust Center
Trusted Publishers
Privacy Options
E-mail Security
Attachment Handling
Automatic Download
Macro Settings
Programmatic Access
Encrypted e-mail
Encrypt contents and attachments for outgoing messages
Add digital signature to outgoing messages
Send clear text signed message when sending signed messages
Request S/MIME receipt for all S/MIME signed messages
Default Setting:
Settings...
Digital IDs (Certificates)
Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.
Publish to GAL...
Import/Export...
Get a Digital ID...
Read as Plain Text
Read all standard mail in plain text
Read all digitally signed mail in plain text
Script in Folders
Allow script in shared folders
Allow script in Public Folders
OK
Cancel

5. Click **OK** to save your settings.

Policy Alerts

This article refers to the Barracuda Message Archiver release 3.1 or higher, except where noted.

Policy Alerts are email notifications that are sent out whenever the Barracuda Message Archiver detects an incoming message that meets the criteria of a Saved Search. This allows you to implement and monitor policies regarding your email traffic, and identify both new and existing messages that meet the specified criteria. You can create local auditor accounts on the Barracuda Message Archiver to negate the need to create temporary users with special access in your corporate directory or email server.

Policy Alert Definitions

The Barracuda Message Archiver includes three built-in policy definitions that are updated as needed by Barracuda Central to meet the latest standards, and are distributed via Energize Updates:

- Personal Email - This policy scans for Personally Identifiable Information such as various formats of drivers' license numbers, credit card numbers, etc.
- Personal Info - This policy scans for foul language words.
- Foul Language - This policy scans for emails sent to and from various sites known by Barracuda Networks to be non-business sites (usually recreation and gambling sites). This policy is designed to alert the administrator when company email is being used for personal and non-business matters.

In addition, you can use any Saved Search to create a new custom Policy Alert from the **POLICY > Alerts** page. You can also modify existing Policy Alerts from this page.

Administrators and auditors can choose to add themselves to the alerts list for these standard policies as well as for any custom Policy Alerts. They are then notified via email either weekly or daily, whenever messages meeting the specified criteria enter into the archive with the offending messages attached to the notification email in a **.zip** file.

Policy Alert Statistics

You can display a count of messages that meet the search criteria of selected Policy Alerts on the **BASIC > Status** page of the Barracuda Message Archiver by enabling the dashboard option when defining the Alert. In addition, you can configure a daily Policy Violations Report containing statistics on all messages that generate a Policy Alert to go out to specific recipients on the **BASIC > Reports** page.

Alert Notification Frequency

From the **POLICY > Alerts** page, specify the alert frequency. In release 3.2 and earlier, you can specify daily or weekly alert notifications. In release 3.5 and higher, you can configure hourly, daily, or weekly alert notifications. For additional configuration options, contact Barracuda Networks Technical Support.

Retention Policies

This article refers to the Barracuda Message Archiver release 3.1 or higher.

While the Barracuda Message Archiver is capable of handling an archive of virtually unlimited size, some organizations may want to expire messages just as a matter of course. The **POLICY > Retention** page allows you to set the maximum age of an archived message before it is permanently purged from the archive. Note that if an auditor has specified an indefinite hold on a Saved Search, the retention policy is treated as an infinite lifetime.

By default, automated purging of messages archived on the Barracuda Message Archiver is disabled. If you enable this ability, the Global Retention Policy and any Saved-Search retention policies are run against all the archived messages once a week.

Warning
If the age of any message exceeds the maximum age allowed by all Saved-Search retention policies that apply to the message, that message is ***permanently deleted from the Barracuda Message Archiver***.

The Global Retention Policy setting does not apply to any messages that match a Saved-Search retention policy.

To enable or disable the automatic message expiration, set the **Allow automatic message deletion** option to *Yes* or *No*.

Global Retention Policy

The Global Retention Policy applies to every archived message. When retention policies are run against the archived messages (once per week), any messages stored on the Barracuda Message Archiver that are older than this age are deleted **unless** they match an existing Saved-Search p olicy.

To configure the Global Retention Policy:

1. Verify that the **Allow automatic message deletion** option is set to *Yes*.
2. In the **Policy Length** field, enter the number of days to retain any archived message.
3. Click **Save Changes**.

Saved-Search Retention Policy

You can define a retention policy based on a Saved Search to automatically delete archived messages from the Barracuda Message Archiver. Note that before you can create a Saved Search retention policy, you must create at least one Saved Search in the **BASIC > Search > Advanced Search** page.

Messages that match the specified Saved Search are permanently removed from the Barracuda Message Archiver when the age of the message exceeds the specified Saved Search policy length.

If you define multiple Saved Search retention policies, if the age of any message exceeds the maximum age allowed by all Saved Search retention policies that apply to the message, that message is permanently deleted form the Barracuda Message Archiver.

Important
Litigation holds overwrite Saved Search and Global Retention Policies; a litigation hold may be for a defined period of time or indefinite.

Automate Message Purging

To run Saved Search retention policies against archived messages, turn on **Allow automatic message deletion**. Once enabled, the Saved Search policies are run against archived messages on a weekly basis each weekend.

Use the following steps to set up a Saved Search retention policy.

1. Log into the Barracuda Message Archiver.
2. Go to the **BASIC > Search** page, and in the **Standard** tab, click **Advanced**.
3. Enter the desired search criteria, and click **Save Search**.
4. Enter the **Search Name**, and click **OK**.
5. Go to the **POLICY > Retention** page, and enter the **Saved Search Retention Policy** details:
    a. In the policy **Name** field, enter a name for the policy you are creating.
    b. In the **Saved Search** field, select the name of the saved search on which this retention policy is to be based.
    c. In the **Policy Length** field, enter the number of days to retain archived messages that match the Saved Search criteria.
6. Click **Add**.

If a message matches more than one Saved Search-based policy, then the message is kept according to the longest policy length. If it matches a Saved Search-based policy as well as the global policy, then the Saved Search policy takes precedence.

Litigation Holds

Litigation Holds are created by auditors to prevent messages that meet the criteria for a specific Saved Search from being removed from the Barracuda Message Archiver. The system administrator must first **Enable Litigation Holds** before auditors will be given the option to create them from the **Saved Searches** tab on the **BASIC > Search** page.

The following information about active Litigation Holds includes:

- **Auditor** - account name of Auditor who created the Litigation Hold
- **Saved Search** - name of the Saved Search associated with the Litigation Hold
- **Hold End Date** - date and time when this Litigation Hold expires

To delete a litigation hold you must have system administrator rights; click the trash can icon following the Litigation Hold you want to delete.

SMTP Proxy

This article refers to the Barracuda Message Archiver release 3.1 or higher.

The Barracuda Message Archiver has the ability to act as an SMTP proxy to directly forward messages to your email server if so desired. The **ADVANCED > SMTP Proxy** page allows you to enter the IP address and TCP port required to allow the Barracuda Message Archiver to forward emails to your email server for delivery.

Important
Because this feature causes the Barracuda Message Archiver to act as a transparent proxy, you must make sure that the mail server to which you are forwarding accepts the sent messages. If message delivery to the next mail destination server fails for any reason (invalid recipient, mail not accepted from the Barracuda Message Archiver's IP address, etc.) then the message is not archived.

Enable Forwarding

To enable forwarding, on the **ADVANCED > SMTP Proxy** page, enter the **IP address** of the desired destination system, and the **TCP port** to be used for communications. For mail servers, the TCP port is the port used for SMTP traffic, typically either 25 or 587. Messages sent to the Barracuda Message Archiver are stored internally prior to being forwarded to the specified destination for further delivery. Leave these fields blank to disable forwarding.

Host Exclusion List

If you have a system such as a Barracuda Spam Firewall that is configured to journal mail to the Barracuda Message Archiver, or if you want to prevent incoming messages from certain systems from being forwarded to another destination even when the proxy feature is enabled, you can pr event forwarding of all messages received from this type of system by entering the IP address in the **Host Exclusion List** field. All messages arriving from sources *not* listed here continue to forward to the destination listed in the **SMTP Proxy Server Configuration** section.

Trusted SMTP Servers

You must enter the IP addresses of all trusted senders of SMTP messages to be archived. On the **MAIL SOURCES > SMTP/IM** page, enter the IP addresses of trusted forwarding servers that will be sending messages to be archived.

Search Options and Configuration

In this Section

- Understanding Message Basics
- Viewing a Message
- Understanding Basic and Advanced Search
- How to Set Up Saved Searches
- Global User Saved Search Filter
- Viewing Search-Related Activities
- Exchange Server 2010 SP1 Shared Mailbox Support
- How to Assign and Unassign PST Files

Additional Resources

- See Tools and Add-Ins for additional search options
- See Auditor Role for auditor Search and configuration options

Related Articles

- Installing and Configuring the Barracuda Message Archiver Outlook Add-In
- Barracuda Message Archiver Mobile Application for iPhone, iPod Touch, and iPad
- Barracuda Message Archiver Mobile Application for Android
- Understanding Email Aliases

Understanding Message Basics

> This article refers to the Barracuda Message Archiver release 3.1 or higher.

You can conduct a search on the following aspects of a message:

- message body content
- recipients and senders
- attachment type and content
- date

Searches can only be made over messages that the searcher has read access to, so privacy is always preserved. Use the Basic Search page for quick one-time searches, or go to the Advanced Search page for a full array of search options including complex search queries and the ability to save searches. Saved Searches are the basis for Policy Alerts, used by Auditors and Administrators to monitor compliance, and Retention Policies, to purge messages from the archiver that are older than a specified date.

Viewing a Message

> This article refers to the Barracuda Message Archiver release 3.1 or higher.

The **BASIC > Search** page of Barracuda Message Archiver initially displays a list of the archived messages that are accessible to the viewing account; only the system administrator has access to all messages in the Barracuda Message Archiver. All other non-admin accounts must be granted access to view messages other than their own.

The Search page displays basic information about a message such as senders and recipients, date, subject, and size. You can view the contents of a message in one of two ways:

- the Preview Pane
- the Message Details window

A single click on any message in the Search results sends it to the embedded Preview Pane for viewing. Double-click on a message to view it in a separate Message Details popup window. Both methods offer the ability to view the message as the sender intended for it to be viewed, as well as the underlying message source code. You can also select the character set to use for a particular message which can be especially useful when viewing a poorly formatted message that does not declare an appropriate charset. You can download each viewable message to your desktop as an .eml file.

Understanding Basic and Advanced Search

This article refers to the Barracuda Message Archiver release 3.1 or higher.

In this article:

- Search Modes
- Basic Search
- Advanced Search

Related Articles

- Advanced Search Options
- Search Options and Configuration

Search Modes

The **BASIC > Search** page offers two search modes, Basic and Advanced:

- **Basic Search** - Run a search based on a word or phrase across all messages accessible by your account
- **Advanced Search** - Run a complex search query based on multiple criteria; note that you can save queries for future use

To switch between the modes, click **Basic** and **Advanced** to the right of the search criteria area.

When you initially go to the **BASIC > Search** page, all messages accessible by your account display in the message list in the **Standard** tab. Both modes are available to all users who have the ability to search through messages, but only the Advanced Search page offers the ability to perform complex queries and create a Saved Search for use in Policy Alerts and Retention Policies.

Administrator Action
New messages received on the Barracuda Message Archiver may not appear in search results for up to 30 minutes because messages are archived and indexed as they are received. If an immediate search is needed across new messages, go to the **BASIC > Administration** page, and click **Reload** in the **System Reload/Shutdown** section.

Basic Search

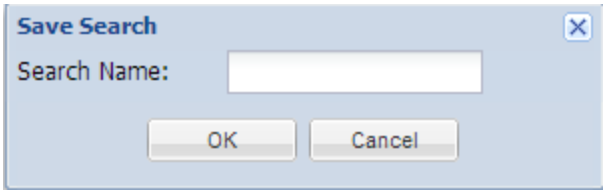
Use the Basic Search mode to perform a quick search across all messages. The Basic Search interface accepts a word or phrase on which to search, and returns all available messages that contain the specified text in either the header or message body. This mode is useful when searching for that handful of emails to or from someone on a specific topic, or when looking for any message that contains a particular phrase. These are one-time searches as these cannot be saved for later use.

Basic Search Term Format
All search terms for Basic Search must be in one of the following formats: **Text-based**, **Multi-Text**, **Wildcards** or **Domain-based**.

Advanced Search

Use the Advanced Search mode to perform complex search queries based on selected attributes. Use the following options to build and save search queries:

- To *add* additional search parameters - Click the plus sign (**+**) to the left of a search criteria line.
- To *remove* a search parameter - Click the minus sign (**-**) to the left of the search parameter you want to remove.
- To *AND* or *OR* search parameters - Once you have more than one search criteria line, the **AND** button displays at the end of each search parameter signifies that it will be logically ANDed to the next specified parameter. If your next criteria is to be logically ORed, click **AND** to toggle it to **OR** and vise versa.
- To *save* a search query - Click **Save Search** below the search criteria; the **Save Search** box displays:



- Enter the name under which the query is to be saved, and then click **OK**. If you enter a name that already exists, the new search parameters replace the previous search criteria.
- To *run* a previously-saved search - Click the **Saved Searches** tab, and click **Search** in the **Actions** column following the Saved Search you want to run.

To receive an alert via email when a message that fits the parameters of a Saved Search is received by the Barracuda Message Archiver, Policy Alerts are required.

Message Actions

This article refers to the Barracuda Message Archiver release 3.5 or higher.

In this article:

- Select Messages
- Resend to Me
- Export Messages
- Forward Messages
- Tag Messages
- Search As User

Related Articles

- Search Options and Configuration
- Advanced Search Options
- Advanced Search Tips

The Barracuda Message Archiver allows you to easily collect messages for exporting or forwarding, and to add tags to messages for future re-identification if desired. You can control whether any or all of these actions are available to users on the **BASIC > Administration** page, in the **Search Page Settings** section.

Messages journaled directly from Microsoft Exchange have additional hidden information, such as bcc recipients and other SMTP data. End-users do not have access to this information; however, for compliance reasons you may want to include this hidden information when messages are exported or forwarded by the administrator or auditor. The **Preserve Journal Wrappers** setting, also in the **Search Page Settings** section, causes the body of an exported or forwarded message to consist of the complete envelope information, with the actual contents of the email turned into an attachment to the message.

If an option is not visible in the Barracuda Message Archiver web interface, the administrator must enable the option on the **BASIC > Administration** page in the **Search Page Settings** section.

Select Messages

The standard selection controls apply when selecting messages in the list view:

- To select *one* message - Single-click on the desired message.
- To select *multiple consecutive* messages - Single-click on a message, and **Shift**-click on another message to select both messages along with all messages listed between those two in the Message List.
- To select *multiple individual* messages - Single-click on one message, and **Ctrl**-click on every other message you want to select.

Resend to Me

To redeliver selected messages to your mailbox, select one or more messages, and then click **Resend to Me** located at the top of the message list,

Export Messages

Once a search is executed and the results are listed in the **BASIC > Search** page, you can choose to export one or more of these messages as a **.pst** or **.zip** file.

To export one or more messages, select the desired item(s) from the message list using **Shift**- or **Ctrl**-click to select multiple messages. Click the **Tools** menu at the top of the message list, and click **Export Messages**. In the window select the desired action and export method. The desired messages are gathered into a single **.pst** or **.zip** file:

- **Export Name** - A label used to identify this export task.
- **Export Type** - The format used to export messages:
  - A single **PST** file suitable for loading into Microsoft Outlook
  - A single **ZIP** file containing individual **.eml** files for each message, with files named under one of the following conventions:
    - **Numerical** - Serial counter, beginning with 0.
    - **Date** - A string of numbers representing the date and time of the message.
    - **Date/From/To** - A (long) string containing the date, time, sender and recipient of the message.
- **Content** - Specify whether to export the **Current Search Results** or **Selected Messages**.
- **Export to -** Select whether to export to the Barracuda Message Archiver for download to your local system, or to a **copy.com** account.

  copy.com
  If you select to save to a copy.com account, you are prompted to enter your copy.com credentials.
- **Chunk Size** - Select the chunk size for the PST or ZIP export as 800MB, 4.7GB, or specify a custom chunk size in gigabytes.

Forward Messages

Once you execute a search and the results display in the **BASIC > Search** page, you can specify one or more of these messages to be forwarded to a desired list of recipients.

To forward one or more messages, select the desired item(s) from the message list using **Shift**- or **Ctrl**-click to select multiple messages. Click on **Tools** located at the top of the message list, and select the desired action. A pop-up dialog prompts you for the email addresses of those users that are to receive the selected messages; use semi-colons to separate multiple email addresses:

- **Forward Selected** - Each message selected in the Message List is individually forwarded (re-delivered) to the specified email address. When this option is selected, a pop-up prompts you for the desired forwarding email address. Use commas to separate multiple delivery destinations.
- **Forward All** - All messages currently in the Message List are individually forwarded (re-delivered) to the specified email address. When this option is selected, a pop-up prompts you for the desired forwarding email address. Use commas to separate multiple delivery destinations.

Tag Messages

Tag messages to easily identify any messages for future use. Tags can be any text, and can be accessed only by the account that created them.

To tag one or more messages, execute a search in the **BASIC > Search** page, and select the desired item(s) from the message list using **Shift**- or **Ctrl**-click to select multiple messages. Click **PSTs & Tags**, click on **Tools** located at the top of the message list, and select the desired Tag action. A pop-up dialog prompts you for the tag text. Tags can then be used as search criteria, allowing you to easily retrieve these messages at a later time:

- **Tag Selected** - Only the messages that have been selected in the Message List are tagged. When this option is selected, a pop-up prompts you for the text with which to tag the messages.
- **Tag All** - All messages currently in the Message are tagged. When this option is selected, a pop-up prompts you for the text with which to tag the messages.
- **Untag Selected** - All tags removed from the selected messages; you cannot remove individual tags on a message.

Search As User

Execute a search across only those messages that are accessible by a specific user. When this option is selected, a pop-up prompts you for the username or email address of the user whose access should be emulated for the search.

Advanced Search Tips

This article refers to the Barracuda Message Archiver release 3.1 or higher.

The search query tips in this article apply to both Basic and Advanced search queries.

- **Searches are performed across only the items to which you have access.** Only messages that are *owned* by you, or those to which your account has been given access either as a *Auditor* or as an administrator, are searched on by your query.
- **All searches are *case insensitive*.** The string *polish* matches both "Polish sausage is not a hot dog" and "Please polish this".
- ***Partial*, or substring, matches are not performed in text-based searches.** If your search string is *age*, it matches only the 3-letter word "age", but not any words containing those three letters in sequence, such as "messages".
- **Wildcards can be used to perform a substring search**, but they **cannot be used as the first character** of a search string. Entering **son* will be the same as entering *son*.
- **Wildcards** may not be used in multi-word phrases even when double-quoted.
- ***Order* does not matter, unless the words are in quotes.** Searching for *meeting room* (no quotes) matches "Meeting in Room 23", "Room 34 is available for your meeting", and "the meeting room is empty". However, entering *"meeting room"* (with quotes) matches only "the meeting room is empty".
- **Certain common English words are ignored.** See the Stop Words section for a complete list of the words that are ignored in searches even when used inside quotes.
- **Wildcard searches also respect Stop Words**, so attaching wildcards to a Stop Word should be avoided since this is the same as if the word was not there at all. Entering *to** does NOT match all words starting with the letters "to" such as "today" and "tomorrow", but is treated as if just * was entered, and therefore matches all words.
- **New messages received on the Barracuda Message Archiver may not appear in search results for up to 30 minutes**. While messages are archived and indexed as they are received, the searchable index is updated every 30 minutes for performance reasons. If an immediate search is needed across new messages, the administrator can go to the **BASIC > Administration** page, and click **Reload** i n the **System Reload/Shutdown** section to update the searchable index with new content.

Advanced Search Options

This article refers to the Barracuda Message Archiver release 3.1 or higher.

In this article:

- Search Parameter All
- Search Parameter Email
- Search Parameter Note
- Search Parameter Appointment
- Search Parameter Distribution list
- Search Parameter Task
- Search Parameter Contact
- Search Parameter Social Media

Related Articles

- Viewing and Searching Messages - Auditor
- Advanced Search Tips
- Search Strings
- Keyword Expressions

Many different actions are possible from the Advanced Search interface that help you to build and save queries with multiple search parameters:

- Add search parameters - Click on the plus sign (+) located to the extreme left of a search criteria line; a new search parameter line is added.
- Remove a search parameter - Click on the minus sign (-) located to the left of the search parameter you wish to remove.
- AND or OR search parameters - Click **AND** at the end of a search parameter to signifies that it is to be logically ANDed to the next specified parameter. If your next criteria is to be logically ORed, click **AND** to toggle it to **OR**.
- Save a constructed query - In the **SAVE AS** field, enter the name under which the query is to be saved, and click **SAVE AS**. If you enter a name that already exists, the new search parameters overwrite the previously saved parameters under that name.
- Run a previously-saved search - Select the Saved Search from the pulldown menu to load the search parameters onto the page, then click **Search**.

Advanced Search Parameters

Select the area of a message to which the search criteria applies.

From the **BASIC > Search** page, click on **Help** for additional search criteria details.

The following tables describe the available advanced search parameters.

Table 1. Search Parameter = All.

Entire Message	Look in all fields and all data contained in each item for the entered text.
Entire Message (Phrase)	Look in all fields and all data contained in each item for the EXACT phrase as entered.
From/Owner	Look only in the **From** and **Owner** fields of each item, as applicable, for the entered text.
Subject	Look only in the **Subject** lines of each item for the entered text. For Distribution Lists, the name of the list is searched. For Contacts, the Full Name (both First and Last) is searched.
Date	Searches for all items with a timestamp that matches the specified date range. For Appointments, the Date is the scheduled start date and time of the Appointment, except when searching Date "is equal to". In that case, the search matches Appointments that span the provided Date. For Tasks, the Date is the date and time that the Task was created.
Archive Time	Searches for all items added to the Barracuda Message Archiver in the specified date range.
Discovery	Searches for all items that were sent or received by any email alias, address, or account that is associated with the specified email addresses, as resolved against the LDAP servers identified on the **USERS > Directory Services** page in the Barracuda Message Archiver web interface. Email addresses must be completely formed (**username@example.com**).

Table 2. Search Parameter = Email.

Entire Message	Look in all fields and all data contained in each item for the entered text.
Entire Message (Phrase)	Look in all fields and all data contained in each message for the EXACT phrase as entered.
Keyword Expressions	Searches based on a custom query using keyword expressions. Each expression must be in the form **search_field:phrase**
Subject/Body	Look only in the Subject line and the body of each message for the entered text.
From/To/Cc	Look only in the **From**, **To**, and **Cc** fields of each message for the entered text.
From	Look only in the **From** field of each message for the entered text.
To/Cc	Look only in the **To** and **Cc** fields of each message for the entered text.
Bcc	Look only in the **Bcc** field of each message for the entered text.
Domain	Look in the **From**, To**,** and **Cc** fields for an email address whose domain matches the entered text.
Subject	Look only in the Subject line of each message for the entered text.

Has Attachment	Returns all messages that have at least one attachment.
Attachment Name	Look only in the names of message attachments for the EXACT phrase as entered.
Contains Images	Returns all messages that contain images embedded in the body.
Image Type	Look for messages with embedded images that are of the specified type. No dot (.) before the extension is needed. For example, enter **gi f to** return all messages that contain images in the **.gif** format.
Inbound	Returns all messages received from an external source by any user in any domain listed in the **Local Domains** section of the **BASIC > IP Configuration** page in the web interface.
Outbound	Returns all messages sent to an external mail server by any user of any domain listed in the **Local Domains** section of the **BASIC > IP Configuration** page.
Internal	Returns all messages sent between any users of any domain listed in the **Local Domains** section of the **BASIC > IP Configuration** page.
Date	Searches for all messages with a timestamp meeting the specified date range. Dates must be entered in the YYYY-MM-DD format.
Body	Look only in the body of the message for the entered text.
Instant Message	Look only in the text of Instant Messages for the EXACT phrase as written.

Table 3. Search Parameter = Note.

Entire Message	Look in all fields and all data contained in each item for the entered text.
Entire Message (Phrase)	Look in all fields and all data contained in each item for the EXACT phrase as entered.
Owner	Look only in the Owner field of the item for the entered text.
Subject	Look only in the Subject line of each item for the entered text.
Date	Searches for all items with a timestamp that matches the specified date range. For Appointments, the Date is the scheduled start date and time of the Appointment. For Tasks, the Date is the date and time that the Task was created.

Table 4. Search Parameter = Appointment.

Entire Message	Look in all fields and all data contained in each item for the entered text.
Entire Message (Phrase)	Look in all fields and all data contained in each item for the EXACT phrase as entered.
From	Look only in the From field of each item for the entered text. For Appointments, the **From** field is usually equivalent to the Organizer of the Appointment, and is the sender or creator of the Appointment.
Subject	Look only in the Subject line of each item for the entered text.

Date	Searches for all Appointments scheduled for the specified time period. Combine two (or more) Date searches to get a list of Appointments scheduled to occur between a specific start and end date.
Location	Look only in the Location field of each item for the entered text.
Attendees	Look only in the Attendees field of each item for the entered text. For Appointments, the **Attendees** field is usually the equivalent of the **To**, **Cc** and **Bcc** fields, and contain the recipients of the Appointment or Meeting Request.

Table 5. Search Parameter = Distribution List.

Entire Message	Look in all fields and all data contained in each item for the entered text. This is the default search scope, and is equivalent to the Basic Search mode.
Entire Message (Phrase)	Look in all fields and all data contained in each item for the EXACT phrase as entered.
Owner	Look only in the Owner field of the item for the entered text.
Subject	Look only at the names of each Distribution List for the entered text.
Date	Searches for all Distribution Lists that were last modified during the specified time period. Dates must be entered in the YYYY-MM-DD format.
Members	Look only in the Members field of each item for the entered text. Matches are based on the individual members' email address as well as their First and Last Names.

Table 6. Search Parameter = Task.

Entire Message	Look in all fields and all data contained in each item for the entered text. This is the default search scope, and is equivalent to the Basic Search mode.
Entire Message (Phrase)	Look in all fields and all data contained in each item for the EXACT phrase as entered.
Delegator (From)	Look only in the From field of each item for the entered text. For Tasks, the From field is usually equivalent to the originator of the Task, and is the sender or creator of the Task.
Subject	Look only in the Subject line of each item for the entered text.
Date	Searches for all Tasks scheduled to end at specified time period. Dates must be entered in the YYYY-MM-DD format.
Assignee (To)	Look only through the owners, of the Task for the entered text. For Tasks, the Owners are usually the equivalent of the To field of a Task Request, and are the ones who are responsible for, or have ownership of, the Task. Matches are based on the attendees' email address as well as their First and Last Names.

Table 7. Search Parameter = Contact.

Entire Message	Look in all fields and all data contained in each item for the entered text. This is the default search scope, and is equivalent to the Basic Search mode.

Entire Message (Phrase)	Look in all fields and all data contained in each item for the EXACT phrase as entered.
Owner	Look only in the Owner field of the item for the entered text.
Name (Subject)	Look only in the Subject of the Contact item for the entered text. This is usually equivalent to the First and Last Names of the Contact.
Date	Searches for all items with a timestamp that matches the specified date range.
Address	Look only in the Address field of each Contact for the entered text.
Email Address	Look only in the Email Address field of each Contact for the entered text.

Table 8. Search Parameter = Social Media.

Entire Message	Look in all fields and all data contained in each item for the entered text. This is the default search scope, and is equivalent to the Basic Search mode.
Entire Message (Phrase)	Look in all fields and all data contained in each item for the EXACT phrase as entered.
Site	Select a social media site from the drop-down list to search for all messages from the selected site.
User	Look only for the user who submitted the social media message.
Date	Searches for all items with a timestamp that matches the specified date range.

Search Strings

This article refers to the Barracuda Message Archiver release 3.1 or higher.

In this article:

- Text-Based Search Strings
- Integer Number-Based Search Strings
- Multi-Text Search Strings
- Wildcards
- Domain-Based Search Strings
- Compound Search Strings
- Stop Words

Related Articles

- Understanding Basic and Advanced Search
- Advanced Search Options
- Keyword Expressions

A *search string* is the format that the searched-for text must be in for searches through the Barracuda Message Archiver. The search query tips in this article apply to both Basic and Advanced search queries.

Text-Based Search Strings

A single string or phrase of text, to be matched exactly as entered. Valid formats are: a single word (with no whitespace) or a single double-quoted sequence of words (separated by spaces). For example:

Sales	Matches "sales guide" but not "Salesmen"

"Reviews due now"	Matches "performance reviews due now" as well as "all reviews are due now" (due to Stop Words being ignored). This does not match "reviews for all employees are due now"

Integer Number-Based Search Strings

A single integer string in bytes to be matched exactly to an index attribute as entered. Valid formats are: a single number (with no whitespace). To find a range, use a Compound Search String. For example:

stored_size:100	Matches all emails with an actual message size on disk of 100 bytes.
size:1536	Matches all emails with a raw size of 1.5KB.

Multi-Text Search Strings

A collection of Text-based words or phrases, separated by spaces. Each item listed must match somewhere, but they do not have to be adjoining or found in the order supplied. For example:

"team meeting" reminder	Matches the phrase "team meeting reminder" as well as the phrase "reminder about the team meeting". This does not match "reminder to the team about the meeting"
"final exam" "open book"	Matches the phrase "The final exam will be open book" as well as the phrase "an open book final exam". This does not match "the final exam is open to anyone with a book"

Wildcards

Wildcards are characters in search strings that can match arbitrary characters in a search. They can ONLY be used as part of a single word, and are NOT allowed as the first character of a search word. They are also NOT allowed in any double-quoted string containing multiple words (i.e., spaces). Wildcards are not allowed as part of a phrase, or any search string that is comprised of more than one word, regardless of the use of double quotes. For example:

nation*	Matches "this nation" and "nationality". This does not match "multinational" or "condemnation"
p???e	Matches any 5-letter word that starts with "p" and ends with "e". This does not match "pore" (only 4 letters), or "pounce" (6 letters)

The question mark (**?**) is a single-character wildcard, matching a single occurrence of any one character. The number of question marks used denote the exact number of characters that must be matched. For example:

luck?	Matches "lucks" and "lucky", but not "luck", "pluck" or "lucked"
J???son	Matches "Johnson" and "Jackson", but not "Jason" or "Judson"

The asterisk (*****) as a multi-character wildcard, matching zero or more occurrences of any and all characters. For example:

Mark*	Matches "marker", "marketing", and "Mark"

Domain-Based Search Strings

The domain part, or everything after the at-sign (@), of an email. For example:

example.com	Matches "*anyuser*@example.com". This does not match "*anyuser*@sub.example.com"
sub2.example.com	Matches "*allusers*@sub2.example.com". This does not match "*allusers*@sub.example.com" or "*allusers*@example.com"

Compound Search Strings

(This is used only in Keyword Expressions.) A combination of two or more strings in any of the above formats (Text-based, Multi-Text, Wildcard or Domain as applicable to the fields being searched) or with other Compound search strings, each separated by the keywords **AND** or **OR**. Surround logical groupings with parentheses as needed to determine order of operations. For example:

subject:(Engineering AND "Meeting today")	Matches items that contain the word "Engineering" as well as the phrase "Meeting today", in any order in the Subject field
body:(Version AND (1.1* OR 1.2*))	Matches items whose body contains, in any order, BOTH the word "version" and a word that starts with either "1.1" or "1.2"
body:((Version AND 1.1*) OR 1.2*)	Matches items that contain a word that starts with "1.2" anywhere in the body of the message, OR items that contain both the word "version" and a word that starts with "1.1", in any order anywhere in the body of the message

Compound search strings of increasing complexity can be constructed by combining multiple compound phrases themselves, to create a single query that identifies multiple search locations in addition to multiple search patterns. For example:

(from:(barracuda.com OR barracudanetworks.com) AND body:datasheets)	Matches all items that were sent from any user in either the "barracuda.com" or "barracudanetworks.com" domains that ALSO contain the word "datasheets" somewhere in the body of the item
((to:user1@mycompany.com AND subject:party) OR (from:user2@yourcompany.com AND subject:gala))	Matches all items sent to **user1@mycompany.com** with the word "party" in the Subject field, as well as all messages from **user2@yourcompany.com** with the word "gala" in the Subject field.

Stop Words

Stop Words are common words that are ignored in searches, and may be omitted.

Recognized Stop Words are:
a, an, and, are, as, at, be, but, by, for, if, in, into, is, it, no, not, of, on, or, such, that, the, their, then, there, these, they, this, to, was, will, with

Stop Words are also ignored in wildcard searches, so make sure that the wildcards are attached to letters that do not comprise a Stop Word in its entirety. For example:

(the AND meeting)	Equivalent to enteringmeeting or "the meeting". This matches both "no meeting minutes" and "the meeting". This does not match "the meetings"
be*	The "be" part is ignored, so this is treated as just * which matches all words

Keyword Expressions

This article refers to the Barracuda Message Archiver release 3.1 or higher, except where noted.

Keyword expressions allow you to construct your own complex queries in Advanced Search, letting you combine multiple keyword-based search terms that follow this basic syntax (without any spaces between the *sear ch_field*, ':', and phrase): ***search_field:phrase***.

In firmware release 3.5 or higher, two additional keyword expressions are available:

- **Keyword proximity syntax form**
- **Fuzzy search syntax form**

Related Articles

- Understanding Basic and Advanced Search
- Advanced Search Options
- Search Strings
- Advanced Search Tips

Commonly used search_field values are listed in the following table:

Term	Description	Search Type
to	Search is limited to the To and Cc fields of each message	Text
from	Search is limited to the From field of each message	Text
domain	Search is limited to the domain names in the From, To, and Cc fields of each message	Domain
subject	Search is limited to the Subject line of each message	Text
body	Searches are performed in the Body of each message as well as in the contents of any message attachments	Text
attachment	Search is limited to the contents of message attachments	Text
all	Searches all fields and all data contained in each message	Text
stored_size	The actual message size on disk	Integer number
size	The raw size of the message	Integer number
header_date	The date header from the mail	Text
header_barracuda_envelope_rcpt_pretty_name	The envelope recipient's pretty name	Text
header_barracuda_envelope_rcpt_user	The envelope recipient	Text
header_to	The To: header	Text
header_in_reply_to	The In reply to: header	Text
header_barracuda_envelope_rcpt_domain	The domain of the envelope recipient	Text
header_from	The From: header	Text
header_barracuda_envelope_rcpt_message_mode	Inbound / Outbound / Internal	Text
header_barracuda_envelope_rcpt_addr	Email address of envelope recipient	Text
header_subject	Subject of the email	Text
header_message_id	The message ID header	Text
object_type	Type of entry (calendar, mail, etc.)	Text
body_excerpt	The body of the email	Text
attachment_name	The attachment name	Text

attachment_mimetype	The attachment MIME type	Text
attachment_extension	The attachment's extension	Text

You may specify other search_field values as long as the correct name for the field is used. Consult Barracuda Networks Technical Support if you are unsure of the exact syntax.

The ***phrase*** can only contain a single item. However, that one item can be any one of the following:

- a single Text-based string;
- a single Integer number-based string;
- a single Wildcarded string;
- a single Domain-based string (*for **to** and **from** search_field only*);
- a single compound search string created by combining multiple strings with the keywords **AND** and **OR**, and grouping the phrases with parentheses to control the logic.

For example:

to:chrislee	All messages that have "chrislee" in the **To** or **Cc** fields.
to:patbrown@mycompany.com	All messages containing "patbrown@mycompany.com" anywhere in the **To** field.
subject:"Barracuda Message Archiver"	All messages that contain the exact phrase "Barracuda Message Archiver" anywhere in the **Subject** line.
domain:(barracuda.com OR barracudanetworks.com)	All messages that were sent to or from any user in either the "barracuda.com" or "barracudanetworks.com" **domain**.
header_barracuda_envelope_rcpt_domain:sub.mycompany.com	All messages sent to any user in the @sub.mycompany.com **domain** .

Proximity Syntax Form (firmware release 3.5 or higher only)

For the keyword proximity syntax form, each ***keyword*** must be in a single Text-based string. Enter the keyword proximity syntax as *search_field:" keyword keyword"~NumericValue,* where *search_field* is the part of the email to search through. For example:

subject:"release Barracuda"~4	All messages containing "release" and "Barracuda" in the Subject field within four words of each other.
to:"Arlo Linda"~6	All messages containing "Arlo" and "Linda" anywhere in the To field within six words of each other.

Fuzzy Search Syntax Form (firmware release 3.5 or higher only)

Fuzzy search allows you to find words that are similar to a specified search term. For the fuzzy search syntax, enter a single keyword followed by the tilde (~). For the fuzzy search syntax form, the *keyword* must be in a single Text-based string.

For example:

roam~	All messages containing words similar to roam, for example, foam, roams.

How to Set Up Saved Searches

This article refers to the Barracuda Message Archiver release 3.1 or higher.

In this article:

- Overview
- Setting Up a Saved Search
- Setting Up a Saved Search Retention Policy

Related Articles

- Saved Searches & Litigation Holds - Auditor
- Policy Alerts - Auditor
- Search Options & Configuration

Overview

Once you execute an Advanced Search, you can save and name the search for re-execution at a later time. A list of all such Saved Searches and their definitions are available on the **BASIC > Search** page in the **Saved Searches** tab, and the search can be performed from this tab.

Any changes to a Saved Search must be done from the **Advanced Search** page by running the Search in question, making the desired changes, and saving the new criteria. Use a new name to create a new Saved Search, or use the existing name to overwrite the previous set of search criteria.

To receive an alert via email when a message that fits the parameters of a Saved Search is received by the Barracuda Message Archiver, Policy Alerts are required.

> You can define a retention policy based on a Saved Search.

Setting Up a Saved Search

1. Log into the Barracuda Message Archiver.
2. Go to the **BASIC > Search** page, and in the **Standard** tab, click **Advanced**.
3. Enter the desired search criteria, and click **Save Search**.
4. Enter the **Search Name**, and click **OK**.
5. Click the **Saved Searches** tab; in this page you can:
   - Click **Search** in the **Actions** column for a Saved Search to immediately run the search.
   - Click **Delete** to remove a Saved Search.
   - Click **Apply/Remove Litigation Hold** to apply or remove a litigation hold for the Saved Search.

Setting Up a Saved Search Retention Policy

1. Go to the **POLICY > Retention** page, and enter the **Saved Search Retention Policy** details:
   - Enter a name for the policy you are creating in the policy **Name** field.
   - In the **Saved Search** field, select the name of the saved search to use for this retention policy.
   - In the **Policy Length** field, enter the number of days to retain archived messages that match the Saved Search criteria.
2. Click **Add**.

> If a message matches more than one Saved Search-based policy, then the message is kept according to the *longest* policy length. If it matches a Saved Search-based policy as well as the global policy, then the Saved Search policy takes precedence.

Global User Saved Search Filter

This article refers to Barracuda Message Archiver firmware 3.5 and higher.

Use Global User Saved Search filter to pre-filter all results before they are displayed to the end-user. For example, the Administrator can restrict all users from viewing emails with the term "Confidential Financials" in the subject. This filter is global, applying to all user sessions.

Use the following steps to specify a Saved Search to automatically filter search results for all accounts with the role **User**.

1. Log in to the Barracuda Message Archiver, and go to the **BASIC > Search** page.
2. Click **Advanced**, enter the desired search criteria, and click **Save Search**.
3. Go to the **BASIC > Administration** page, and in the **Search Page Settings** section, select the desired Saved Search from the drop-down menu.

4. click **Save Changes**. The specified saved search is added to every user's default search filter.

Viewing Search-Related Activities

This article refers to the Barracuda Message Archiver release 3.1 or higher.

In this article:

- Audit Log Page
- Filter Options
- Results Pane

Related Articles

- Audit Log Filtering

Audit Log Page

The **ADVANCED > Audit Log** page of Barracuda Message Archiver displays a list of all search-related activities that have been performed on the Barracuda Message Archiver. In this view you can browse through the list, or perform a search to filter on a subset of activities. You can filter by start/end dates, user name, and item type. Click on an activity to display the activity details in the **Details** pane.

Filter Options

When the Audit Log page is loaded, no filter options are set by default, and all audit log records display. Using filtering options, you can monitor a specific date range, a specific action type, a specific user, or you can combine criteria. Unlike the Search page, you may only specify at most one criterion per criteria type, and all specified criteria are always ANDed together. Leave any criterion blank to allow all possibilities. You can specify the following criteria:

- **Start Date** - Use the date-picker to choose a date to form half of a date range. If **Start Date** is specified, no results earlier than that date display in the results. Leave this field blank (or delete its contents) to view results with no restriction on how old they may be.
- **End Date** - Use the date-picker to choose a date to form half of a date range. If **End Date** is specified, no results later than that date display. Leave this field blank (or delete its contents) to view results with no restriction on how recent they may be.
- **User** - Enter a user name to view only actions performed by that user. As you type in this field, a list of matching users displays from which you can select. Leave this field blank (or delete its contents) if you wish to filter by all users. If a user is not displayed in the drop-down menu, then that user may not have performed any actions which have been recorded in the Audit Log.
- **Type** - Select an action type from the drop-down menu to view only actions of that specific type. Select blank to not filter by type, i.e. to view results of any action type. If a type is not displayed in the drop-down menu, it may be that no actions of that type have been performed, or that action is not tracked in the Audit Logs.

Once you have entered the filter criteria, click **Search** to return Audit Log results matching your criteria.

You may specify **Start Date** and **End Date** by typing in a date, instead of using the date-pickers. If you do so, you must specify the date in the following format - "YYYY-MM-DD". If you use an invalid format, an error message displays when you click **Search** . Additionally, if you enter an invalid date range (that is, **End Date** comes before **Start Date**), an error message displays when you click **Search** .

Results Pane

The **Results Pane** displays audit log records matching the search criteria. Information displayed for each record includes:

- **Date** - When this action occurred and was logged in the Audit Log
- **User** - Which user performed this action; some actions are performed by the Barracuda Message Archiver automatically, not actively by a specific user. These actions will have the user "System" displayed for them.
- **Type** - What type of action this record is for. For instance, when a user logs in, a "Login" action appears, and when a user instructs the Barracuda Message Archiver to import a PST, a "PST Import" action appears.
- **Detail** - Many audit log records contain information in addition to the date, user, and type. In some cases, a useful piece of this additional information is displayed in the **Detail** column, for instance, to narrow down a broad action type.
- **Details Pane** - Many audit log records contain information in addition to the date, user, and type. To view this additional information, click on that record's row; a pane displays the record details. The additional information that is available varies by action type, and sometimes within a given type.

The **Results Pane** also lets you navigate through large quantities of results, via the **Page Navigation** controls in the upper-left corner. Additionally, you can customize the look of the pane using the **Tools** menu.

The options in the **Tools** menu are:

- **Results Per Page** - Choose how many rows of audit log results display per page in the **Results Pane**. If there are more results than can fit on one page, you can always use the **Page Navigation** controls to view them.
- **Details Pane** - Choose which side of the **Results Pane** the **Details Pane** is to appear. Options are **Right**, **Bottom**, and **Left**.

Exchange Server 2010 SP1 Shared Mailbox Support

This article refers to Barracuda Message Archiver firmware 3.5 and higher, and Microsoft® Exchange Server 2010 SP1 with shared or delegate mailboxes.

In this article:

- Understanding Shared Mailbox Support
- User Search
- Shared Mailbox Configuration
- Shared Mailbox Support - Auto-Mapping Enabled
- Shared Mailbox Support - Auto-Mapping Disabled

Related Articles

- Microsoft Exchange Server 2010 Deployment

Additional Resource

- Mailbox Auto-Mapping in Exchange Server 2010 (Part 1)
- Mailbox Auto-Mapping in Exchange Server 2010 (Part 2)

Understanding Shared Mailbox Support

The Barracuda Message Archiver's Shared Mailbox Support feature allows a Barracuda Message Archiver user access to email based upon Microsoft Exchange Server's shared mailbox capability.

User Search

When a user searches for emails in the Barracuda Message Archiver web interface, Barracuda Message Archiver Outlook Add-In, or through a Barracuda Message Archiver Mobile Application, the search results include emails from both the user's mailbox as well as all mailboxes shared with that user.

Shared Mailboxes
Shared mailboxes and their folders display in the Barracuda Message Archiver web interface. However, shared PSTs are not supported at this time.

Shared Mailbox Configuration

On your Exchange Server you can create a shared mailbox for use by multiple users. For Exchange Server 2010 SP1 and higher, the Barracuda Message Archiver supports shared mailboxes when one of the following is true:

- A user is assigned full access permissions to another mailbox via the Exchange Management Console (EMC). This action populates the LDAP attribute **MSExchDelegateListLink**, and is used to determine shared mailbox access.
- A user is assigned delegate access to another mailbox via Microsoft Outlook. This action populates the LDAP attribute **PublicDelegates**, and is used to determine shared mailbox access.

Conversely, the Barracuda Message Archiver does not support shared mailboxes if **Send As** permissions are enabled from the EMC. This action *does not* populate any LDAP fields, preventing the Barracuda Message Archiver from determining shared mailbox access.

Shared Mailbox Support - Auto-Mapping Enabled

Shared mailbox support is easily available when auto-mapping is enabled. Auto-mapping is typically enabled by default on Exchange Server 2010 SP1 and higher.

> **Auto-Mapping Disabled**
> If you are not using auto-mapping, you must create attributes in Active Directory (AD) to enable shared mailbox support as described in the section **Shared Mailbox Support - Auto-Mapping Disabled**.

Shared Mailbox Support - Auto-Mapping Disabled

If auto-mapping is disabled on the Exchange Server, specific AD attributes that the Barracuda Message Archiver uses to determine shared mailbox details may not exist. Therefore, to ensure shared mailboxes function properly, you must manually create specific AD attributes. The Barracuda Message Archiver uses either the **MSExchDelegateListLink** or **PublicDelegates** AD attributes for a user to determine what mailboxes are being shared.

Exchange Server 2010 SP1 Shared Mailbox Support Auto-Mapping

This article refers to Barracuda Message Archiver firmware 3.5 and higher, and Microsoft® Exchange Server 2010 SP1 with shared or delegate mailboxes.

Shared Mailbox Support - Auto-Mapping Enabled

Shared mailbox support is easily available when auto-mapping is enabled.

> **Auto-Mapping Disabled**
> If you are not using auto-mapping, you must define attributes in Active Directory (AD) to enable shared mailbox support as described in the section **Shared Mailbox Support - Auto-Mapping Disabled** .

If auto-mapping is not enabled, use the following PowerShell command:

1. Log in to the Exchange 2010 Server with an account that is authorized to use PowerShell.
2. On the Server, go to **Start > All Programs > Accessories > Windows PowerShell > Windows PowerShell**.
3. Run the following command in Remote PowerShell:
   `Add-MailboxPermission "`*`Shared Mailbox`*`" -User "`*`User`*`"`
   `-AccessRights FullAccess`
   Where *`Shared Mailbox`* is the shared mailbox name, and *`User`* is the name of the user to which you wish to assign permissions.
4. Auto-mapping is now enabled.

Shared Mailbox Support - Auto-Mapping Disabled

The Barracuda Message Archiver determines shared mailbox details through AD look-ups. The Exchange auto-mapping feature (Exchange 2010 SP1 and higher) automatically populates the required AD attributes. If auto-mapping is disabled on the Exchange Server, the Exchange Administrator can manually populate the needed AD entries. Use the following rules when setting up your Exchange Server/AD workflow:

The Barracuda Message Archiver supports shared mailboxes when one of the following is true:

- A user is assigned full access permissions to another mailbox via the *Exchange Management Console*. This action populates the LDAP attribute`MSExchDelegateListLink`, and is used to determine shared mailbox access.
- A user is assigned delegate access to another mailbox via *Outlook*. This action populates the LDAP attribute `PublicDelegates`, and is used to determine shared mailbox access.

Conversely, the Barracuda Message Archiver *does not* support shared mailboxes if **Send As** permissions are enabled from the *Exchange Management Console*. This action *does not* populate any LDAP fields, preventing the Barracuda Message Archiver from determining shared mailbox access.

> **Shared Mailboxes**
> Shared mailboxes and their folders display in the Barracuda Message Archiver web interface. However, shared PSTs are not supported at this time.

User Search

When a user searches for emails in the Barracuda Message Archiver web interface, Barracuda Message Archiver Outlook Add-In, or through a Barracuda Message Archiver Mobile Application, the search results include emails from both the user's mailbox as well as all mailboxes shared with that user.

How to Assign and Unassign PST Files

This article refers to the Barracuda Message Archiver release 3.1 or higher.

In this article:

- Assign a PST File to a User
- Unassign a .pst File

Related Articles

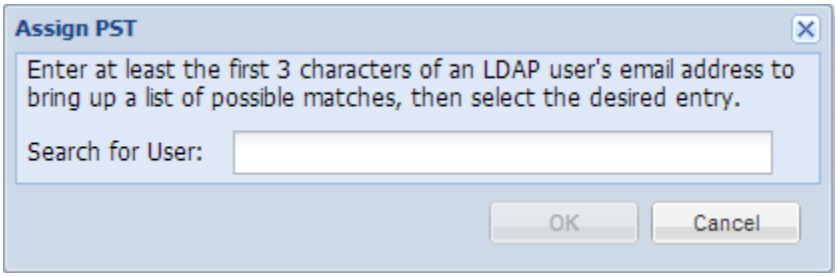
- Barracuda PST Collector
- Search Options & Configuration

All imported PST files must be manually assigned to an account before its contents can be accessed by that account. Only one account can be assigned to every PST file, but multiple PST files can be assigned to any account. For details on initial PST file import to the Barracuda Message Archiver, refer to the Barracuda PST Collector deployment options.

Assign a PST File to a User

Use the following steps to assign a PST file to an LDAP user and make the contents searchable from within the Barracuda Message Archiver:

1. Log in to the Barracuda Message Archiver web interface, go to the **BASIC > Search** page, and click the **PSTs & Tags** tab.
2. Expand **PSTs**, and then expand the **Unassigned PSTs** folder.
3. Right-click on a PST file, and click **Assign PST**.
4. In the **Assign PST** dialog box, enter the first few characters of either the username or the email address of the user to which to assign the PST file:


Assign PST
Enter at least the first 3 characters of an LDAP user's email address to bring up a list of possible matches, then select the desired entry.
Search for User:
OK
Cancel

5. As you type in the user field, matching users display in a drop-down list. Select the user to which to assign the PST file, and click **OK**.

   The list of users populates based on your LDAP directory; you can only assign a PST file to a user found in the list.

6. The PST file now displays in the **Assigned PSTs** folder under the selected user name.

You can also assign a PST file by dragging it to a specific user listed in the **Assigned PSTs** folder.

Unassign a .pst File

To unassign a PST file, complete either of the following actions:

- Right-click the PST file and click **Unassign PST**; the PST displays in the **Unassigned PSTs** folder
- Click and drag the PST file to the **Unassigned PSTs** folder

Monitoring

In this Section

- Viewing Performance Statistics
- Setting Up Alerts
- Viewing System Tasks
- Understanding the Front Panel Indicator Lights
- Reports

Viewing Performance Statistics

This article refers to the Barracuda Message Archiver release 3.1 or higher.

In this article:

- Message Statistics
- Performance Statistics
- Policy Statistics
- Storage Statistics
- Subscription Status
- Cluster Status
- Hourly and Daily Statistics

The **BASIC > Status** page provides an overview of the health and performance of your Barracuda Message Archiver, including:

- Traffic and policy statistics, such as the amount of overall email traffic and how many messages have triggered a particular policy category.
- The subscription status of Energize Updates.
- Performance statistics including CPU temperature and system load. Performance statistics displayed in red signify that the value exceeds the normal threshold. These values fluctuate based on the amount of traffic that is being handled. However, if any setting remains consistently in the red for a long period of time, contact Barracuda Networks Technical Support.

Message Statistics

Statistics for all items stored on the Barracuda Message Archiver, broken down into the following groups by hour, day, and total:

- Inbound, outbound, and internal emails
- Appointments, contacts, notes, and tasks
- Any other data belonging to users in your managed domains that were also sent to the Barracuda Message Archiver

Performance Statistics

(Not available to auditors)

The Performance Statistics section displays information on the current operating status and performance of the Barracuda Message Archiver including:

- System load, CPU fan speed and temperature, and system fan speed and temperature
- Firmware storage and mail/log storage
- Redundancy (RAID)
- Index queue length and last message archived
- Cloud Control

Policy Statistics

Statistics for all built-in policy alerts and the policies chosen on the **POLICY > Alerts** page for listing on the dashboard. Details regarding each of the Policies listed can be found on the **POLICY > Alerts** page.

To choose which policies to display in this table, go to the **POLICY > Alerts** page (or click **Policy Definitions**), and select the **Dashboard** check

box for the desired policies.

Storage Statistics

(Not available to auditors)

This section displays statistics on the amount of data stored on the Barracuda Message Archiver this hour, today (since midnight), and total (or since last reset).

- **Effective** - The "real" combined size of all messages stored on the Barracuda Message Archiver. This is the actual size of the messages as they are sent to the Barracuda Message Archiver.
- **On Disk** - The actual amount of storage used on the Barracuda Message Archiver.
- **Reduction** - The percentage of storage space saved by the compression mechanisms of the Barracuda Message Archiver.

Subscription Status

(Not available to auditors)

This section displays the current status of your Energize Updates subscription, and the optional Instant Replacement andPremium Support subscriptions. If the status displays as *Warning* or *Expired*, please contact your reseller or Barracuda Networks to update your subscription(s).

Cluster Status

(Not available to auditors)

The number of messages awaiting processing on this Barracuda Message Archiver and its high availability (HA) pair if one has been configured from the **ADVANCED > High Availability** page.

Hourly and Daily Statistics

The breakdown of message traffic and policy violations for the last 24 hours and last 30 days.

Setting Up Alerts

> This article refers to the Barracuda Message Archiver release 3.1 or higher, and the Barracuda Message Archiver model 450 or higher.

In this article:

- SNMP Alerts
- Emailed System Alerts
- SNMP Manager
  - Setting Up SNMP Manager
  - MIB and REF Files

SNMP Alerts

The Barracuda Message Archiver 450 and higher offers the ability to monitor various settings via SNMP including:

- Traffic and policy statistics, such as:
  - Amount of overall traffic;
  - Number of messages that triggered a particular policy category;
  - Number of messages currently in the indexing queue.
  - The subscription status of Energize Updates.
- Performance statistics, including CPU temperature and system load.

Emailed System Alerts

Use the **BASIC > Administration** page to configure the Barracuda Message Archiver to automatically email notifications to specified addresses; use a comma to separate multiple addresses.

System alerts notify you when:

- Your Energize Updates subscription is about to expire

- Possible backup, synchronization, Journal account, or other connectivity failures
- Your system is low on disk space

SNMP Manager

You can use the SNMP Manager to query system information.

Setting Up SNMP Manager

Use the following steps to set up SNMP Manager,

1. Log into the Barracuda Message Archiver web interface, and go to the **BASIC > Administration** page.
2. In the **SNMP Manager** section, set **Enable SNMP Agent** to *Yes*. This setting allows the Barracuda Message Archiver to accept and respond to SNMP queries.
3. Select the **SNMP Version** as either **v2c** or **v3**; select the **v3** protocol for a more secure transmission.
    a. If you select **v2c**, enter the **SNMP Community String** to allow the Barracuda Message Archiver to communicate SNMP information; the default string used by the Barracuda Message Archiver is **cudaSNMP**
    b. If you select **v3**, enter the SNMP username and password, and select the authentication and encryption methods.
    c. In the **Allows SNMP IP/Range** section, enter the **IP Address** and **Netmask**, or click **Bulk Edit** to enter multiple entries in the form: IP Address,Netmask Note: If no IP address or network is specified, then SNMP access is possible from any system.
    d. Click **Add**.

MIB and REF Files

Once you set up the SNMP Manager, import the following MIB and REF files to your SNMP monitor (note that these files are standard across all Barracuda Networks products):

- The Barracuda Message Archiver MIB
- The Barracuda Reference MIB (standard across all Barracuda Networks products)

You can monitor objects included in these MIB and REF files either from custom scripts or from your SNMP monitor. The MIB files are located on the Barracuda Message Archiver and can be obtained by replacing *MGMTIP* in the following links with the management IP address of your Barracuda Message Archiver:

- http://*MGMTIP*:8000/Barracuda-BMA-MIB.txt
- http://*MGMTIP*:8000/Barracuda-REF-MIB.txt

Viewing System Tasks

> This article refers to the Barracuda Message Archiver release 3.1 or higher.

The **ADVANCED > Task Manager** page provides a list of tasks that are in the process of being performed, and displays any errors encountered when performing these tasks.

Some of the tasks that the Barracuda Message Archiver tracks include:

- Imports of historical emails
- Exports of archived messages
- Configuration restoration

If a task takes a long time to complete, you can click the **Cancel** link next to the task name and then run the task at a later time when the system is less busy.

The **Task Errors** section lists an error until you manually remove it from the list; errors are not phased out over time. Any task that results in an error is listed in the **Task Errors** section, with a red Error Summary link to this list present on every page in the UI as long as there are errors in this list. Click on the **Clear** link to remove errors, since all errors remain in this list until explicitly removed.

Understanding the Front Panel Indicator Lights

The Barracuda Message Archiver has five indicator lights on the front panel that blink when the system processes any message.

Light	Color	Description
-	Red	*Reserved for future use*
-	Yellow	*Reserved for future use*

Traffic	Green	Blinks when the Barracuda Message Archiver processes traffic.
Data I/O	Green	Blinks during data transfer.
Power	Green	Displays a solid green light when the system is powered on.

Reports

This article refers to the Barracuda Message Archiver release 3.1 and higher, except where noted.

In this article:

- Email Activity Report
- Top Storage Users Report
- Policy Violations Report
- Global Searches Report
- Usage Report *(Available only in Release 3.2 and Higher)*
- Generate Reports
  - Show Report
  - Email Report
- Daily Report Email Options
- Report Properties

The built-in reports on the Barracuda Message Archiver provide statistics on various operational, legal, and storage aspects. Default reports include message archive growth, policy violations, archive traffic, and cost analysis and projected archive storage growth.

On the **BASIC > Reports** page you can generate the following reports:

- **Email Activity Report** - View Barracuda Message Archiver email activity by user
- **Top Storage Users Report** - View Barracuda Message Archiver storage usage by user
- **Policy Violations Report** - View Barracuda Message Archiver email policy violations by user
- **Global Searches Report** - View the top Barracuda Message Archiver global searches by user
- **Usage Report** *(available in release 3.2 and higher)* - Generate an overview of Barracuda Message Archiver cost analysis and projected archive storage growth

Email Activity Report

This report displays the total number of emails by user for the specified date range. The report displays a list of all users and their email count as well as a graphical representation based on the **Chart Type** selection in the **Report Properties** section.

Top Storage Users Report

This report displays a list of top storage users and the total storage each user has used on the Barracuda Message Archiver. Specify the maximum number of users you wish to display in the report by entering a value in the **Top Count** field in the **Report Properties** section. When the report is generated, the report displays a list of the top storage users based on the value in the **Top Count** field, the total storage used by each, and a graphical representation of usage based on your **Chart Type** selection in the **Report Properties** section on the **BASIC > Reports** pa ge.

Policy Violations Report

This report displays a list of policies and the number of times that a policy was violated within the specified date range. This report includes custom policies, and all built-in policies when enabled on the **POLICY > Alerts** page. When the report is generated, the report displays the number of times the policies were violated within the selected date range. Additionally, a graph displays the data based on your **Chart Type** selec tion in the **Report Properties** section on the **BASIC > Reports** page.

Global Searches Report

This report displays a list of all global searches performed within the specified date range by users with the *admin* or *auditor* role. This report includes the global search criteria, the user who performed the search, and the number of times the global search was performed. Additionally, a graph displays the number of times each global search was performed based on your **Chart Type** selection in the **Report Properties** section on the **BASIC > Reports** page.

Usage Report (Available only in Release 3.2 and Higher)

This report displays a comprehensive report of archiving activity, cost savings, and projected storage growth based on U.S. dollars per gigabyte for the selected date range. For additional information, see Barracuda Message Archiver Usage Report.

Generate Reports

On the **BASIC > Reports** page you can generate individual reports on a one-time basis by specifying the desired **Report Type** and **Date Range**. You can select to either email the generated report to one or more recipients, or view the report on-screen.

> Because report generation can consume a large amount of resources, particularly if the requested report covers a long time period and/or has to process a large amount of data, *reports for a time span of longer than 7 days can only be generated for email delivery*.
>
> Note that **Show Report** is not available when generating a Usage Report.

Show Report

Click **Show Report** to generate and view a report onscreen. Note that the date range cannot exceed seven days to view the report onscreen. To generate a report that covers more than a seven-day period, use the **Email Report** function.

Email Report

To send an email containing the selected report to a specific user, select the report type, specify the date range, enter an email address in the **Email Report to** field, and then click **Email Report**. A message displays at the top of the page noting that the report is generating and will be sent to the specified user.

Daily Report Email Options

You can optionally set up automatic report generation of email activity, top storage users, policy violations, and global searches in the **Automated Reports** section on the **BASIC > Reports** page. Enter one or more recipients to have a report emailed daily to one or more users.

Report Properties

In the **Report Properties** section on the **BASIC > Reports** page you specify how the report content is presented. You must click **Save Changes** for these values to be used in daily reports defined in the **Automated Reports** section.

Barracuda Message Archiver Usage Report

> This article refers to the Barracuda Message Archiver release 3.2 or higher.

You can view a comprehensive report of archiving activity, cost savings, and projected storage growth based on U.S. dollars per gigabyte.

Go to the **BASIC > Report** page, and in the **Generate Report** section, select **Usage Report** from the **Report Type** drop-down menu:

- Specify the desired date range
- Enter the email address to which to send the report

Click **Email Report** to generate and send the report to the specified email address. The report is attached to the email as a PDF file.

The PDF report displays the following details:

- **PDF Header** - Barracuda Message Archiver hostname, serial number, and report generation date.
- **Yearly Summary** - Displays a summary of employee hours saved, total storage savings in U.S. dollars, and the number of emails flagged for policy violations.
- **Archiving Activity** - Displays email, non-email, and messages flagged by policy in table format, as well as a summary pie chart:
  - Total inbound, outbound, and internal archived email by week, month, and year
  - Total non-email items archived including appointments, contacts, notes, and tasks by week, month, and year
  - Total number of emails flagged by built-in and custom policies by week, month, and year
- **Access** - Displays the total logins, exports, and search access by week, month, and year, as well as estimated time savings in hours per weekday:
  - **Access Overview** - displays total user login, export, search activity
  - **Administrator** - displays login, export, and search activity for administrator role only
  - **Auditor** - displays login, export, and search activity for auditor role only

    - **User** - displays user login, export, and search activity for web interface, Outlook Add-In, and Mobile App (excluding Administrator and Auditor roles)
- **Storage** - Displays message stubbing and PST management details:
    - **Microsoft Exchange Stubbing** - Displays the total messages stubbed, storage savings, and cost savings by week, month, and year
    - **PST Management** - Displays the total number of uploaded PST files, PST storage size, and cost savings by week, month, and year
    - **Capacity and Retention Policy Management** - Displays the projected yearly growth, time until expected saturation, and retention rate storage based on current usage, device size, and current retention rates including a storage utilization graph with projected cumulative yearly storage

Maintenance

In this Section

- Configuration Backups
- Updating Your Firmware and Definitions
- Replacing a Failed System
- Reloading, Restarting, and Shutting Down the System
- Troubleshooting
- How to Reboot the System in Recovery Mode
- Migrating to a New Barracuda Message Archiver

Configuration Backups

> This article refers to Barracuda Message Archiver firmware version 3.1 or higher.

The contents of an existing configuration backup file can be restored onto the Barracuda Message Archiver, whether the backup file was created manually or automatically. To restore a backup of all your stored email data from a data backup you made onto your network via a means as described in the article Understanding Archived Data Backup, contact Barracuda Networks Technical Support. Your raw emails and additional content (additional content available for restoration varies with firmware revision) can then be moved to your Barracuda Message Archiver from your backup by Barracuda Networks Technical Support.

From the **Restoring Backups** section, you can upload either a desktop backup or an automated backup for restoration.

Related Articles

Firmware 3.5 and higher:

- How to Back Up Your Archived Data
- Understanding Archived Data Backup

Firmware 3.2 or earlier

- How to Back Up Your Barracuda Message Archiver

To restore a backup file:

1. Identify the backup file to restore:
    - **Restore Backup File** - Enter the path and name of a locally-available backup file. This is generally used to restore a backup saved on your local system or file share. Click **Browse** to navigate to the file location.

- **Restore Auto Backup** - Path and name of the automatically-created backup file. Click **Browse** to open a window with a list of all currently available backup files currently in the location specified in the **Automated Backups** section.

2. Click **Upload**; a confirmation screen displays a list of items in the backup file that are to be restored.
3. Click **Apply Now** to begin the restoration.

> If the restore is being done to transfer settings onto a new and unconfigured Barracuda Message Archiver, be sure to manually set the IP address and DNS information under **BASIC > IP Configuration**.

Restoring to a New Barracuda Message Archiver

If you are restoring a backup file on a new Barracuda Message Archiver that is not yet configured, you must assign your new system an IP address and DNS information on the **BASIC > IP Configuration** page.

Note the following about the backup file:

- Do not edit backup files. Any configuration changes you wish to make must be done through the Web interface. The configuration backup file contains a checksum that prevents the file from being uploaded to the system if changes are made.
- You can safely view a backup file in Windows WordPad or Microsoft Word; avoid viewing backup files in Windows Notepad because the file can become corrupted if you save the file from this application.
- The following information is not included in the backup file:
  - System password
  - System IP information
  - DNS information

Updating Your Firmware and Definitions

This article refers to the Barracuda Message Archiver release 3.1 or higher.

Updating Your Barracuda Message Archiver Firmware

Use the **ADVANCED > Firmware Update** page to manually update the firmware version of the system or revert to a previous version. The only time you should revert back to an old firmware version is if you recently downloaded a new version that is causing unexpected problems. In this case, call Barracuda Networks Technical Support before reverting back to a previous firmware version.

If you have the latest firmware version already installed, the **Download Now** button is disabled.

> **Important**
> Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours.

Updating the Definitions from Energize Updates

The **ADVANCED > Energize Updates** page allows you to manually update the Virus, Policy, and Document Definitions used on your Barracuda Message Archiver, as well as to change the interval at which the Barracuda Message Archiver checks for updates.

It is recommended that you set the **Automatically Update** to **On** so that your Barracuda Message Archiver receives the latest rules as soon as they are available by Barracuda Central.

Replacing a Failed System

This article refers to the Barracuda Message Archiver release 3.1 or higher.

Related Articles

- How Barracuda Networks Manages Returned Device Drives
- Removing or Replacing a System in a High Availability Configuration
- Migrating to a new Barracuda Message Archiver

Before you replace your Barracuda Message Archiver, use the tools provided on the **ADVANCED > Troubleshooting** page to try to resolve the problem.

In the event that a Barracuda Message Archiver fails and you cannot resolve the issue, customers that have purchased the Instant Replacement service can call Barracuda Networks Technical Support and arrange for a new unit to be shipped out within 24 hours.

After receiving the new system, ship the old Barracuda Message Archiver back to Barracuda Networks at the address below with an RMA number clearly marked on the package; Barracuda Networks Technical Support can provide details on the best way to return the unit.

> Barracuda Networks, Inc.
> 3175 S. Winchester Blvd
> Campbell, CA 95008
>
> attn: RMA # *<your RMA number>*

Reloading, Restarting, and Shutting Down the System

> This article refers to the Barracuda Message Archiver release 3.1 or higher.

The **System Reload/Shutdown** section on the **BASIC > Administration** page allows you to shutdown, restart, and reload system configuration on the Barracuda Message Archiver.

Shutting down the system powers off the unit. Restarting the system reboots the unit. Reloading the system re-applies the system configuration.

You can perform a hard reset of the Barracuda Message Archiver by pressing the **RESET** button on the front panel of the system. Take caution when pressing the reset button as doing so while the Barracuda Message Archiver is in the midst of a configuration update or other task can result in inadvertent corruption of the system.

Troubleshooting

> This article refers to the Barracuda Message Archiver release 3.1 or higher.

The **ADVANCED > Troubleshooting** page provides various tools to help troubleshoot network connectivity issues that may impact the performance of your Barracuda Message Archiver.

For example, you can test the connection of your Barracuda Message Archiver to the Barracuda Networks update servers to verify that it can successfully download the latest Energize Updates definitions. You can also ping other devices from the Barracuda Message Archiver, perform a trace-route from the Barracuda Message Archiver to any another system, and execute various other troubleshooting commands.

How to Reboot the System in Recovery Mode

> This article refers to the Barracuda Message Archiver release 3.1 and higher.

If your Barracuda Message Archiver experiences a serious issue that impacts its core functionality, you can use diagnostic and recovery tools available at the reboot menu to return your system to an operational state.

Before using the diagnostic and recovery tools, do the following:

- Use the built-in troubleshooting tools on the **ADVANCED > Troubleshooting** page to help diagnose the problem.
- Perform a system restore from the last known good backup file.
- Contact Barracuda Networks Technical Support for additional troubleshooting tips.

As a last resort, you can reboot your Barracuda Message Archiver and run a memory test or perform a complete system recovery, as described below.

To perform a system recovery or hardware test:

1. Connect a monitor and keyboard directly to your Barracuda Message Archiver.
2. Reboot the system by doing one of the following:
   - Click **Restart** on the **BASIC > Administration** page.
   - Press the **Power** button on the front panel to turn off the system, and then press the **Power** button again to turn the system back on.
3. The Barracuda splash screen displays with the following three boot options:
   ```
   Barracuda
   Recovery
   Hardware_Test
   ```

4. Use your keyboard to select the desired boot option, and press **Enter**.

Important
You must select the boot option within three seconds of the splash screen appearing. If you do not select an option within three seconds, the Barracuda Message Archiver defaults to starting up in the normal mode (first option).

To stop a hardware test, press **Ctrl-Alt-Del** to reboot your Barracuda Message Archiver.

Reboot Options	Description
Barracuda	Starts the Barracuda Message Archiver in the normal (default) mode. This option is automatically selected if no other option is specified within the first three (3) seconds of the splash screen appearing.
Recovery	Displays the Recovery Console where you can select from the following options: • **Perform file system repair** - Repairs the file system on the Barracuda Message Archiver. • **Perform full system re-image** - Restores the factory settings on your Barracuda Message Archiver, and clears out all configuration information. • **Enable remote administration** - Initiates a connection to Barracuda Central that allows Barracuda Networks Technical Support to access the system. Another method for enabling this troubleshooting connection is to click **Establish Connection to Barracuda Networks** on the **ADVANCED > Troubleshooting** page. • **Run diagnostic memory test** - Runs a diagnostic memory test from the operating system. If problems are reported when running this option, it is recommended that you next run the Hardware_Test option.
Hardware_Test	Performs a thorough memory test that shows most memory-related errors within a two-hour time period. The memory test is performed outside of the operating system and can take a long time to complete. Reboot your Barracuda Message Archiver to stop the hardware test by pressing **Ctrl**-**Alt**-**Del**.

Migrating to a New Barracuda Message Archiver

Important

Consult your Barracuda Networks Product Specialist before migrating from an existing Barracuda Message Archiver to a new Barracuda Message Archiver model, or contact Barracuda Networks Technical Support.

If you are replacing a failed system, contact Barracuda Networks Technical Support, or refer to Replacing a Failed System.

If you are deploying your Barracuda Message Archiver with a Microsoft® Exchange Server and are planning to migrate to a newer version of Exchange Server, or if you plan to change the Barracuda Message Archiver local hostname in an existing Exchange Server deployment, refer to the article Barracuda Message Archiver and Microsoft Exchange Server Migration.

If you have purchased a new Barracuda Message Archiver and need to migrate your data from the old unit, this work is performed by Barracuda Networks Technical Support.

Your raw emails and the metadata that has been built about your emails (searchable index, statistics, etc) will be moved to your Barracuda Message Archiver from your backup by Barracuda Networks Technical Support. In the event that after a local catastrophe you need to move data from a backup you prepared to a replacement Barracuda Message Archiver, contact Barracuda Networks Technical Support. See Understanding Archived Data Backup for information on how to back up your Barracuda Message Archiver for fastest recovery from a disaster.

Tools and Add-Ins

Go to the **USERS > Client Downloads** page in the Barracuda Message Archiver to download Tools and Add-Ins.

In this Section

- Barracuda Message Archiver Outlook Add-In
- Barracuda Message Archiver Mobile Applications
- Barracuda PST Collector
- Barracuda Message Archiver Stand-Alone Search Utility

Related Articles

- Creating an Email Service Account for Microsoft Exchange Server 2003
- Creating an Email Service Account for Microsoft Exchange Server 2007, 2010, and 2013

Barracuda Message Archiver Outlook Add-In

In this Section

- Barracuda Message Archiver Outlook Add-In Deployment
- Installing and Configuring the Barracuda Message Archiver Outlook Add-In
- How to Search and Archive Messages Using the Barracuda Message Archiver Outlook Add-In
- Troubleshooting the Barracuda Message Archiver Outlook Add-In
- How to Enable the Barracuda Message Archiver Outlook Add-In in a Microsoft Terminal Server Environment
- Barracuda Outlook Add-In Customization Options
- How to Create Local Mailstores

Barracuda Message Archiver Outlook Add-In Deployment

This article refers to the Barracuda Message Archiver release 3.1 or greater, and the Barracuda Message Archiver Outlook Add-In Version 3.1 or greater. The Barracuda Message Archiver Outlook Add-In supports Outlook versions 2003, 2007, 2010, and 2013.

Verify the Outlook Add-In version (available for download on the **USERS > Client Downloads** page) is the *same major revision* as the Barracuda Message Archiver firmware for proper functionality.

In this article:

- Locale
- Installation
- Configuration Options
- Configure Using Administrative Templates
    - Administrative Template Deployment Options
    - Outlook 2010 or Outlook 2013 64-Bit Support
    - Administrative Template Deployment Testing
    - Administrative Template Deployment Troubleshooting
- Configure Using DNS

Related Articles

- Outlook Add-In Installation and Configuration
- Outlook Add-In Customization Options
- Outlook Add-In Troubleshooting

Secure Connectivity
The Barracuda Message Archiver Outlook Add-In requires secure (HTTPS) connectivity to the Barracuda Message Archiver. If an insecure (HTTP) connection is attempted the Outlook Add-In is redirected to use *https:* with the configured secure port (the default port is 443).

For existing Outlook Add-in users, if your URI was originally set up via Group Policy on an earlier firmware version, verify that the URI uses HTTPS. If the URI was set up using HTTP, use the steps in the section **Configure Using Administrative Templates** to update the URI. If the URI is *not* updated, users are automatically redirected to the secure, HTTPS protocol. This redirection may require an update to your network firewall rules to allow connectivity to complete on the secure port.

Microsoft Office Click-to-Run for Office 2010
If you are running Microsoft Office Click-to-Run for Office 2010, Microsoft has reported that the environment has potential issues when running Add-Ins such as the Barracuda Message Archiver Outlook Add-In. As a result, the Barracuda Message Archiver Outlook Add-In may not function as expected. For additional information, refer to the Microsoft Knowledgebase article Office 2010 Click-to-Run compatibility with add-ins.

Windows Server 2003 Deployment
If you are deploying the Outlook Add-In from Windows Server 2003 to Windows Vista or later, you must disable User Account Control (UAC) on the client workstations because UAC is not supported in Windows Server Group Policy (GPO) deployments prior to Windows Server 2008. If UAC is not disabled, you will encounter an error similar to the following:

```
Module C:\Windows\systems32\BmaPST32.dll failed to register. HRESULT -2147023782. contact your support personnel
```

For more information on managing UAC through GPO, refer to the Microsoft Knowledgebase article UAC Group Policy Settings and Registry Key Settings.

Locale

The language for the Barracuda Message Archiver Outlook Add-In options is determined by your Microsoft Office installation locale. Supported languages for the Add-In include:

- English
- Spanish (Continental)
- French
- Japanese
- Dutch
- Italian
- Chinese

Installation

Use the following steps to install the Barracuda Message Archiver Outlook Add-in Deployment Kit.

1. Log into the Barracuda Message Archiver as an administrator.
2. Navigate to the **USERS > Client Downloads** page, and download the **Outlook Add-In Deployment Kit**.
3. Extract the contents to an easily accessible location; the deployment kit contains the following:
   - Barracuda Message Archiver Outlook Add-in installer for Outlook 2010 or Outlook 2013 64-bit (**BmaOutlookAddIn-*version*_x64.msi**)

- Barracuda Message Archiver Outlook Add-in installer for all other versions of Outlook (**BmaOutlookAddIn-*version*_x86.msi**)
- Barracuda Message Archiver Outlook Add-in Administrator module (**Barracuda Message Archiver Outlook Add-In *version*.adm**)

4. Move (or copy) the **Barracuda Message Archiver Outlook Add-In *version*.adm** file to your local %systemroot%\inf directory typically found in: c:\winnt\inf
5. Copy the **.msi** file(s) to a location that is accessible by your users.
6. Open the Group Policy Object (GPO) Editor for the organization that is to use the Barracuda Message Archiver Outlook Add-in (e.g., the default domain policy).
7. If you do not already have a network share for GPO software deployment, you must create one. The share must be accessible from all of the machines on which the software is to be deployed. The permissions for the share must give read access to the "Everyone" group, and the permissions for the underlying NTFS folder must give read access to the "Authenticated Users" group.

   The software is installed by the *machines* themselves rather than by users, and machines are not members of the "Everyone" group, therefore this modification to the default permissions is required.

8. Either *edit* the default policy, or *create* a new policy object, then link it to the desired container. For example, the particular OU containing the computers on which the add-in is to be installed.
9. Expand **User Configuration**, right-click **Administrative Templates**, select **All Tasks**, and click **Add/Remove Templates**.
10. Navigate to %systemroot%\inf, select **Barracuda Message Archiver Outlook Add-In *version*.adm**, and click **Add**.

Configuration Options

You can configure the Barracuda Outlook Add-In through Administrative Template (ADM) files, or through DNS.

The Add-In is configured based on the following order of precedence:

1. User-configured URL, *unless*
2. ADM is configured to set the ADM-configured URL to take precedence;
3. ADM-configured URL;
4. DNS-configured hostname.

Configure Using Administrative Templates

Use the following steps to configure the Barracuda Message Archiver Outlook Add-in.

1. While still in the GPO Editor, navigate to **User Configuration > Administrative Templates**, and expand the Barracuda node that should now be visible.
2. Click **Message Archiver**, and click **Barracuda Message Archiver Outlook Add-In**.
3. Double-click the **Barracuda Message Archiver URI** policy, and enter the fully qualified URI that Outlook users are to use to access the Barracuda Message Archiver (e.g., `https://archiver.mycompany.com:443`).
   Note the following:
   - If users will be accessing the Barracuda Message Archiver from outside the local network, the URI must be externally accessible.
   - HTTPS is required when connecting from Outlook, specify 'HTTPS' in the URI.
   - Remember to include the port number in the URI. If you have not changed the default port settings on your Barracuda Message Archiver, the HTTPS port is 443.
   - By default users can enter a different URL to connect to other than one specified here; turn on **Require Users to Use Configured URL** to disable this field and enforce usage of the specified URL.
4. Configure other settings as required. For an explanation of the available settings, click the **Explain** tab in the policy.

Administrative Template Deployment Options

Use the following steps to deploy the Microsoft installer (MSI) file.

1. Start the GPO Editor for the domain where you will be installing the Outlook Add-In.
2. Either *edit* the default policy or *create* a new policy object, and link it to the desired container; for example, the particular OU containing the computers of users that will be using the add-in.
3. Navigate to **Computer Configuration > Software Settings > Software Installation**, right-click **Software Installation**, and select **New/Package**.
4. Enter the UNC path to the .msi file located in the shared folder, and click **OK**.

Outlook 2010 or Outlook 2013 64-Bit Support

If you have both 32-bit and 64-bit machines in your environment, but *none* of the 64-bit machines are running Outlook 2010 or Outlook

2013 64-bit, the x86 version of the MSI is recommended for deploying the add-in by default to all 32-bit as well as 64-bit machines. However, if there are some 64-bit machines that have Outlook 2010 or Outlook 2013 64-bit installed, then there are three possible deployment scenarios.
Scenario 1

Every 64-bit machine in your environment has Outlook 2010 or Outlook 2013 64-bit installed.

Click to view Scenario 1

In this case, perform *all* of the following steps:

1. Go to the **Deployment** tab for the 32-bit package.
2. Click **Advanced**, and uncheck the **Make this 32-bit x86 application available to Win64 machines** option.
3. Repeat steps 1 through 4 specified in the Administrative Template Deployment Options section above for the 64-bit MSI.

The 32-bit MSI is deployed only to 32-bit machines, and the 64-bit MSI is deployed only to 64-bit machines.

Scenario 2

Some 64-bit machines in your environment have Outlook 2010 or Outlook 2013 64-bit installed while others have the 32-bit version of various other Outlook versions installed, *and* Outlook was installed through a GPO.

Click to view Scenario 2

In this case, perform ***all*** of the following steps:

1. Apply the policy you created in the steps described in the Scenario 1 section above only to those computers that were targeted for the installation of 32-bit Outlook.
2. Repeat steps 1 through 4 specified in the Administrative Template Deployment Options section above for the 64-bit MSI, and apply this second policy *only* to those computers that were targeted for the installation of Outlook 2010 or Outlook 2013 64-bit.

The 64-bit MSI is installed only on those computers where Outlook 2010 or Outlook 2013 64-bit is installed, and the 32-bit add-in is installed on all other computers to which the policy has been applied.

Scenario 3

The 64-bit machines in your environment have a mixture of Outlook 2010 or Outlook 2013 64-bit and other 32-bit versions of Outlook installed, *but there are no existing AD containers* that specify on which of these computers Outlook 2010 or Outlook 2013 64-bit is installed.

Click to view Scenario 3

In this case, perform ***only one*** of the following:

- Manually create and populate these AD containers and then perform the steps in **Scenario 2**; *or*
- Consider installing Outlook 2010 or Outlook 2013 32-bit on all computers (unless you have users that require the 64-bit capabilities of Office 64-bit); *or*
- Manually install the correct version of the add-in on each machine; *or*
- Allow your users to install the correct version of the add-in installer for themselves (they must have administrative privileges on their computers).

Administrative Template Deployment Testing

Complete the following steps to test the Barracuda Message Archiver Outlook Add-in deployment.

> Group Policy updates can take several minutes to post; run `gpupdate /force` to perform an immediate update.

1. Restart a computer that is joined to the domain.
2. Verify that the Add-In is installed when you log in, and that the configured policies are applied.

Administrative Template Deployment Troubleshooting

Following is a list of troubleshooting tips:

- A common cause of failure is that the user and/or the user's computer does not have adequate access to the share location. Verify that all access and network privileges are configured appropriately.
- Additional error messages are available in the Event Log on the domain computer; if you do not find the desired information in the Event Log, consider enabling verbose logging and restarting the computer.
- For additional information on fixing Group Policy issues, see Fixing Group Policy problems by using log files on the Microsoft technet website.

Configure Using DNS

Use the following steps to create an SRV record in the form:
`_barracuda_ma._tcp.[AD domain]`

1. On the DNS server, click **Start**, click **Administrative Tools**, click **DNS**.
2. Expand the tree until the domain displays, for example, archiver.local, right-click on the domain name, click **Other New Records**.
3. In the dialog, select the resource record type **Service Location (SRV)**, and click **Create Record**.
4. From the **Service** drop-down menu, select: **_barracuda_ma**
5. From the **Protocol** drop-down menu, select: **_tcp**
6. Click **Port Number**, and enter the port number; if you do not enter a port number, port 443 is used by default.
7. In the **Host offering this service** field, enter the AD domain of the Barracuda Message Archiver, for example: **archiver.domain.local**
8. Click **OK**, and then click **Done**.
9. Under the domain name in the left pane, click **_tcp**; the SRV record displays in the list in the center pane.

When using a DNS-configured hostname to configure the Barracuda Message Archiver Outlook Add-In, HTTPS is always used.

Installing and Configuring the Barracuda Message Archiver Outlook Add-In

This article refers to the Barracuda Message Archiver release 3.1 or greater except where noted, and the Barracuda Message Archiver Outlook Add-In version 3.1 or greater. The Barracuda Message Archiver Outlook Add-In supports Outlook versions 2003, 2007, 2010, and 2013.

Verify the Outlook Add-In version (available for download on the **USERS > Client Downloads** page) is the *same major revision* as the Barracuda Message Archiver firmware for proper functionality.

In this article:

- Locale
- Installation
- Configuration
- Configuration Options
- Changing the URI (Location)
- Attachment and Whole-Message Stubbing
- Message Stubbing Options
- Restore Stubbed Content to Microsoft Exchange
- Folder Synchronization
- Manual Folder Content Synchronization

Related Articles

- Outlook Add-In Search and Archive
- Outlook Add-In Deployment
- Outlook Add-In Troubleshooting
- Mobile Application for iPhone, iPod Touch, and iPad
- Mobile Application for Android

Secure Connectivity
The Barracuda Message Archiver Outlook Add-In requires secure (HTTPS) connectivity to the Barracuda Message Archiver. If an insecure (HTTP) connection is attempted the Outlook Add-In is redirected to use *https:* with the configured secure port (the default port is 443).

For existing Outlook Add-in users, if your URI was originally set up via Group Policy on an earlier firmware version, verify that the URI uses HTTPS. If the URI was set up using HTTP, use the steps in the **Changing the URI (Location)** section to update the URI. If the URI is *not* updated, users are automatically redirected to the secure, HTTPS protocol. This redirection may require an update to your network firewall rules to allow connectivity to complete on the secure port.

Important - Microsoft Office Click-to-Run for Office 2010
If you are running Microsoft Office Click-to-Run for Office 2010, Microsoft has reported that the environment has potential issues when

running Add-Ins such as the Barracuda Message Archiver Outlook Add-In. As a result, the Barracuda Message Archiver Outlook Add-In may not function as expected. For additional information, refer to the Microsoft Knowledgebase article Office 2010 Click-to-Run compatibility with add-ins.

Message Archive and Search
For Search and Archive options, refer to How to Search and Archive Messages Using the Barracuda Message Archiver Outlook Add-In.

The Barracuda Message Archiver Outlook Addin allows you to perform various functions with messages that are stored on your organization's Barracuda Message Archiver, including:

- Synchronization of your archived folders with Outlook
- Search for archived messages and other Microsoft Outlook data, such as Contacts
- View and interact with (forward, reply to, etc.) all of your archived Outlook items
- Access stubbed attachments
- Archive messages

These functions are available directly from within Outlook, allowing transparent access to your messages and attachments, all with no browser interaction required. All that is needed is a network connection to your organization's mail server and to the Barracuda Message Archiver.

Locale

The language for the Barracuda Message Archiver Outlook Add-In options is determined by your Microsoft Office installation locale. Supported languages for the Add-In include:

- English
- Spanish (Continental)
- French
- Japanese
- Dutch
- Italian
- Chinese

Installation

(Barracuda Message Archiver Administrator only)

As the Barracuda Message Archiver administrator, you can install the Outlook Add-in in one of two ways:

- **Outlook Add-In Deployment Kit** - Go to the **ADVANCED > Client Downloads** page and click **Download Now** to download the deployment kit which includes all files necessary to perform a GPO deployment of the Barracuda Message Archiver Outlook Add-In, for both 32- and 64-bit versions of Outlook (refer to the Barracuda Message Archiver Outlook Add-In Deployment Guide for more information)
- **Outlook Add-In Installer** - Go to the **ADVANCED > Client Downloads** page and click **Download Now** to download an executable for installing the Add-in on a system to enable access to the Barracuda Message Archiver form directly inside either a 32- or 64-bit version of Outlook

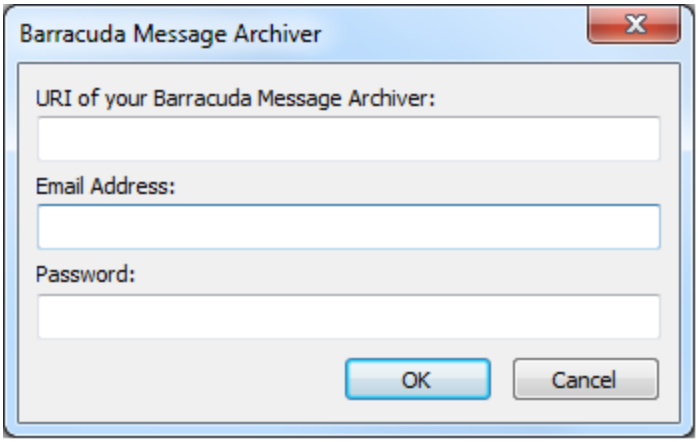
Configuration

Typically, the preconfigured Barracuda Message Archiver Outlook Add-in settings do not require any modification. However, in some instances a Barracuda Message Archiver location configuration screen may display, or you may wish to adjust message stubbing frequency or caching. You adjust these settings through the Barracuda Message Archiver **Options** dialog box.

Initial Log In

The first time you use the Barracuda Message Archiver Outlook Addin, you are prompted to enter your login credentials:

- URI of your Barracuda Message Archiver - The URI generally starts with https:// followed by the system name or IP address, and may end with a colon ":" and a number, for example: `https://archiver.company.com:8000`
- Your complete email address, for example, `myname@company.com`
- Your domain (LDAP) password, typically your email password



Once you enter these details and click **OK**, Microsoft Outlook automatically remembers your login credentials, and there is no need to enter this information again unless you change your password. If you forget your password or are unable to access the Barracuda Message Archiver Outlook Addin, contact your system administrator.

> **Important**
> If your organization configures local users on the Barracuda Message Archiver, each user receives a Barracuda Message Archiver User Rollout email. If the login credentials differ from your email address, please use the account information provided in the Rollout email to log into the system.

Barracuda Message Archiver Options Dialog Box

Use the following steps to access the **Barracuda Message Archiver Options** dialog box: The location of the **Options** dialog box is based on your version of Microsoft Outlook:

- If you are using Outlook 2003 or 2007, go to **Tools > Options > Barracuda Networks**, and click **Options**:

- If you are using Outlook 2010 or 2013, click the **File** tab, click **Barracuda Networks** in the list, and click **Configure**:

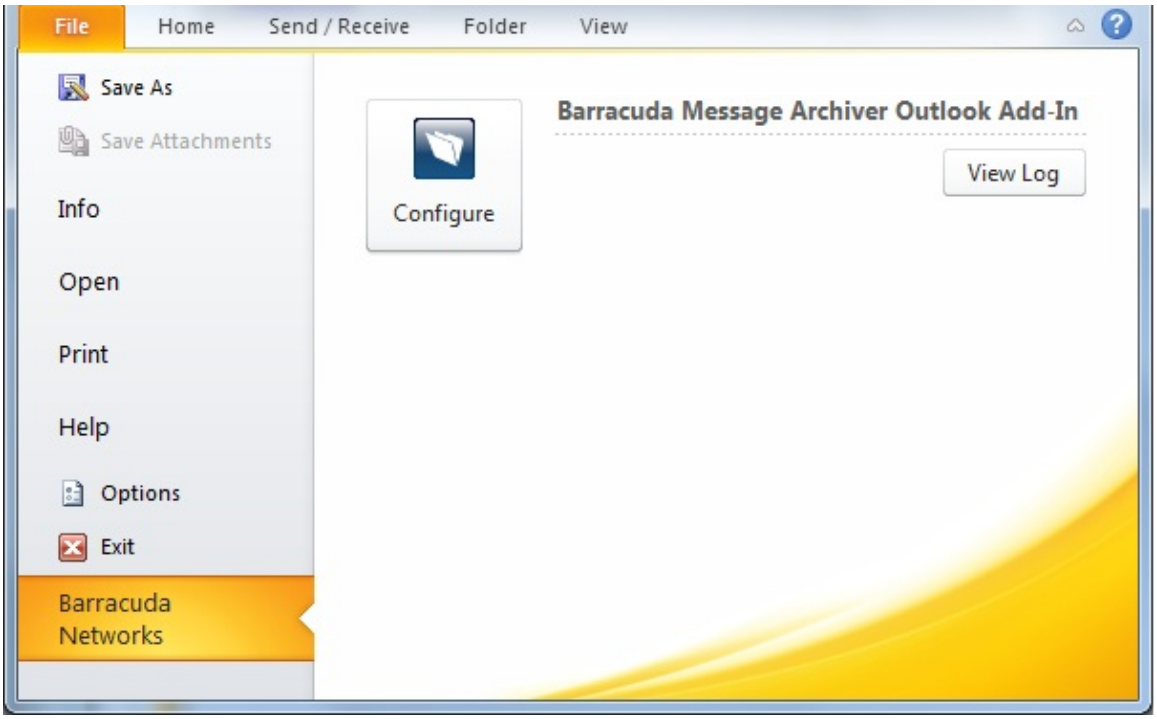
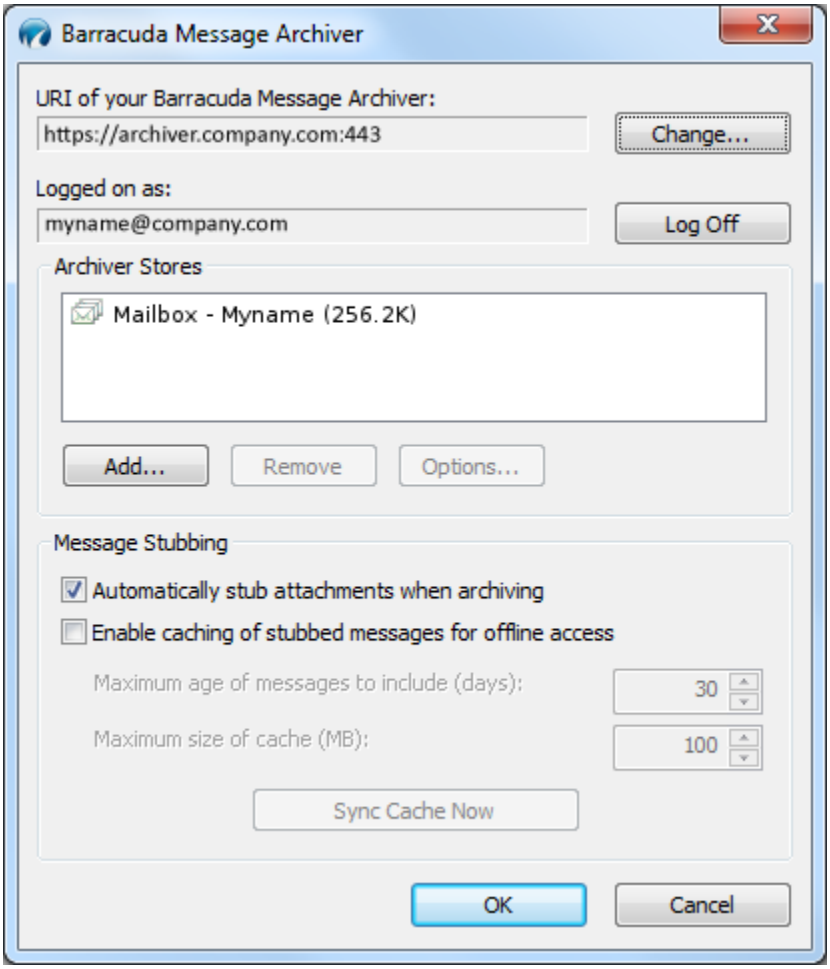


Figure 1. Barracuda Message Archiver Options dialog box.



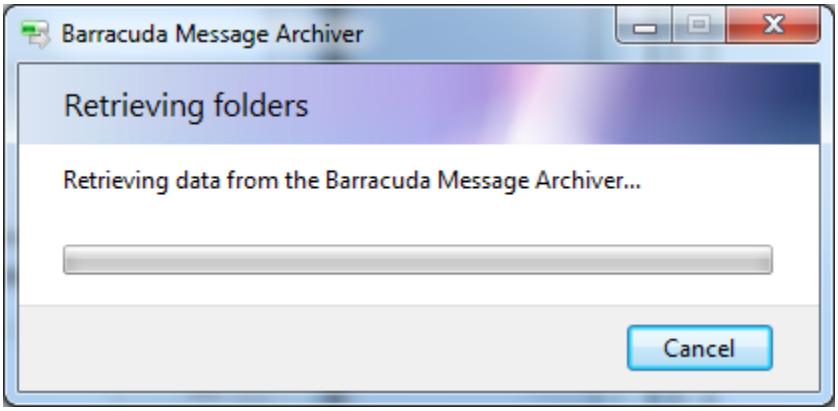
Configuration Options

In the **URI/Logged on as** sections, you can configure the following options:

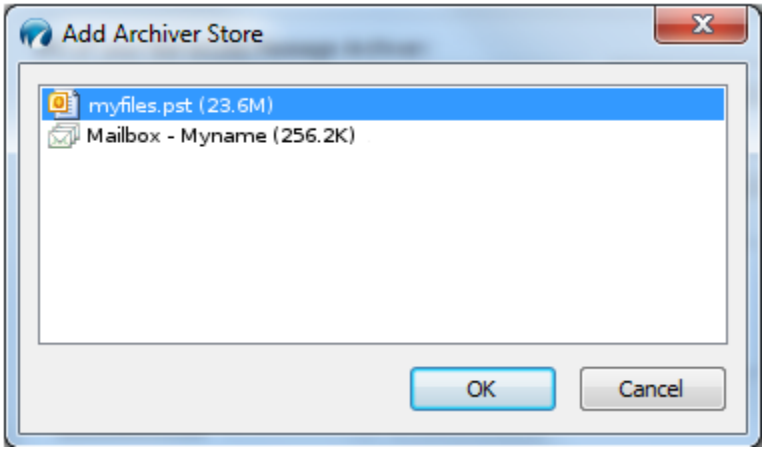
- **Change** - Click to change the Barracuda Message Archiver URI and user access details. For more information, see the Changing the URI (Location) section.
- **Log Off** - Click to log out the current user.
- **Archiver Stores** - This section displays the Barracuda Message Archiver stores (Mailboxes) to which you have access.

> **Firmware Version**
> Note that you must have Barracuda Message Archiver release 3.1 or greater to search through folder hierarchy in PST files within the Barracuda Message Archiver web interface.

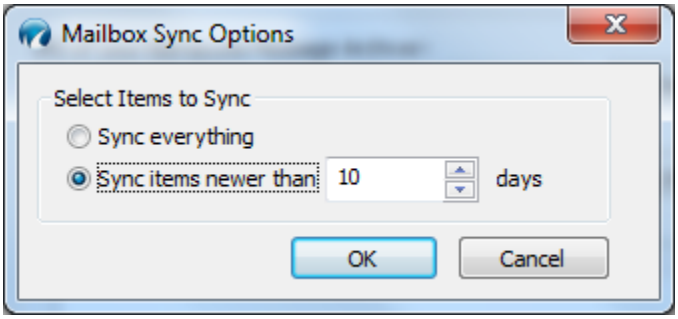
  - **Add** - Click to select additional stores:



Once the folders are retrieved, Archiver Stores to which you have access, and that are not already being synchronized, display. Select the store you wish to add, and click **OK**:



  - **Remove** - Click on a store in the list, and then click **Remove** to remove it from the list of available stores
  - **Options** - Click on a store in the list, and then click **Options** to open the **Mailbox Sync Options** dialog box and specify the desired synchronization settings:



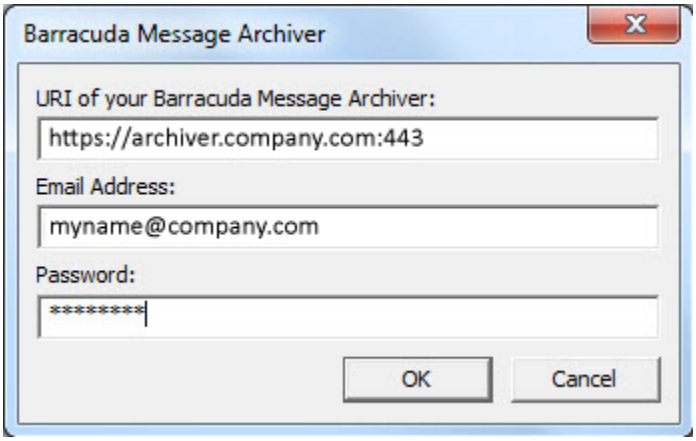
> Specify the number of days in the **Sync items newer than** field to govern how often messages are deleted and the period of time messages are stored. Messages older than this value are deleted, and messages newer than this value are synchronized and saved. Set this value to a lower number to reduce synchronization time and reduce the size of the store.

- In the **Message Stubbing** section, you specify message stubbing options. For a description of each option, see the **Message Stubbing Options** section.

Changing the URI (Location)

If you need to change the location of your Barracuda Message Archiver, first contact your system administrator for the correct URI, and then use the following steps.

1. In the **Barracuda Message Archiver Options** dialog box, click **Change** to display the dialog box:



2. Replace the Barracuda Message Archiver URI with the new location provided by your system administrator, for example: `https://archiver.newcompanyname.com:443`
3. If your email address or password has changed, enter your email address and password in the associated fields.

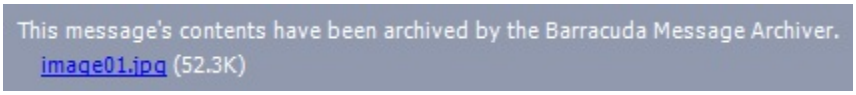
> If you received a Barracuda Message Archiver User Rollout email, enter the credentials provided in the email.

4. Click **OK**. Microsoft Outlook automatically remembers your login credentials.

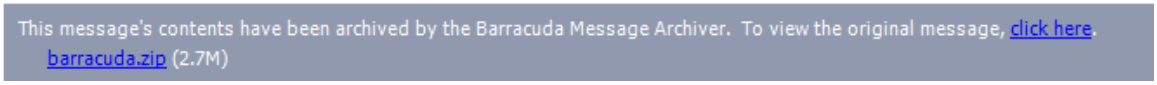
Attachment and Whole-Message Stubbing

Message stubbing options are defined by the Barracuda Message Archiver administrator on the **MAIL SOURCES > Exchange Integration** page.

When a message *attachment* is stubbed, the attachment is removed from the message and is replaced with an attachment indicator and a link to the preserved attachment:



When an *entire* message is stubbed, the message body is replaced with a text excerpt and contains a link to the original message:

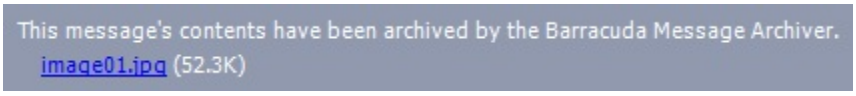

This message's contents have been archived by the Barracuda Message Archiver. To view the original message, click here.
barracuda.zip (2.7M)

Message Stubbing Options

Use the **Barracuda Message Archiver Options** dialog box to specify message stubbing options.

Automatically Stub Attachments when Archiving

This option allows all incoming messages containing attachments to be stubbed as soon as the message is submitted to the Barracuda Message Archiver. All attachments are still accessible directly from within the actual message; the only difference is that the attachment itself is stored on the Barracuda Message Archiver instead of your organization's Outlook server. The email contains the following text with a link to the attachment:



Click on the attachment name to view and download the attachment directly from the Barracuda Message Archiver to your local system.

Enable Caching of Stubbed Messages for Offline Access

This option allows a copy of stubbed attachments to be stored locally on your system. This allows you to retrieve the attachment when you do not

have direct access to the Barracuda Message Archiver.

Maximum Age of Messages to Include (Days)

Maximum age (number of days) of mail that will be copied to the local workstations stub cache.

Maximum Size of Cache (MB)

Use this option to specify the maximum amount of disk space, specified in megabytes (MB), on your local computer to use for caching stubbed attachments. When the cache is full, the oldest items in the cache are removed from your local system in order until there is enough space for the newest items. Note that these attachments are still stored on, and accessible from, the Barracuda Message Archiver.

Synchronize Cache Now

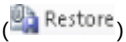
When selected, initiates a connection to the Barracuda Message Archiver to update your local cache of stubbed messages immediately instead of waiting for the next scheduled synchronization (as determined by your system administrator).

For example, if you are accustomed to downloading your messages from your mail server before leaving on a road trip, you can synchronize your cache immediately to ensure that any attachments associated with your messages can always be retrieved.

Important
You can click **Synchronize cache now** to verify connectivity to the **Barracuda Message Archiver**.

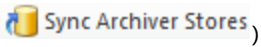
Restore Stubbed Content to Microsoft Exchange

Firmware Version
This feature is available only in the Barracuda message Archiver Outlook Add-In version 3.2.30 and higher.

To restore stubbed content to your Microsoft Exchange Server, click the **Restore** (

) icon in the Outlook toolbar. When clicked, the selected stub content is restored to the Exchange Server and persists on the Server for 30 days.

Folder Synchronization

When items are syncing, a system tray icon displays until synchronization is complete. When synchronization is successful and is scheduled, there is no notification and no further action is needed. However, if a problem is encountered, or if the user clicks the **Sync Archiver Stores** (

) icon on the toolbar, a tooltip displays additional information.

Store synchronization occurs when either the user clicks the **Sync Archiver Stores** (

) icon, after nightly synchronization jobs are complete, or shortly after Outlook is started.

Manual Folder Content Synchronization

Firmware Version
This feature is available only in the Barracuda message Archiver Outlook Add-In version 3.2 and higher.

To manually synchronize all folder content on the Barracuda Message Archiver, click the **Sync Archiver Stores** (

) icon in the Outlook toolbar.

How to Search and Archive Messages Using the Barracuda Message Archiver Outlook Add-In

This article refers to the Barracuda Message Archiver release 3.1 or greater except where noted, and the Barracuda Message Archiver Outlook Add-In version 3.1 or greater, except where noted. The Barracuda Message Archiver Outlook Add-In supports Outlook versions 2003, 2007, 2010, and 2013.

Verify the Outlook Add-In version (available for download on the **USERS > Client Downloads** page) is the *same major revision* as the Barracuda Message Archiver firmware.

In this article:

- Searching
  - Search Criteria
  - Advanced Search Criteria
- Message Results
- Archiving Messages
- Applying a Category to Archived Items
- Restoring Stubbed Content to Microsoft Exchange

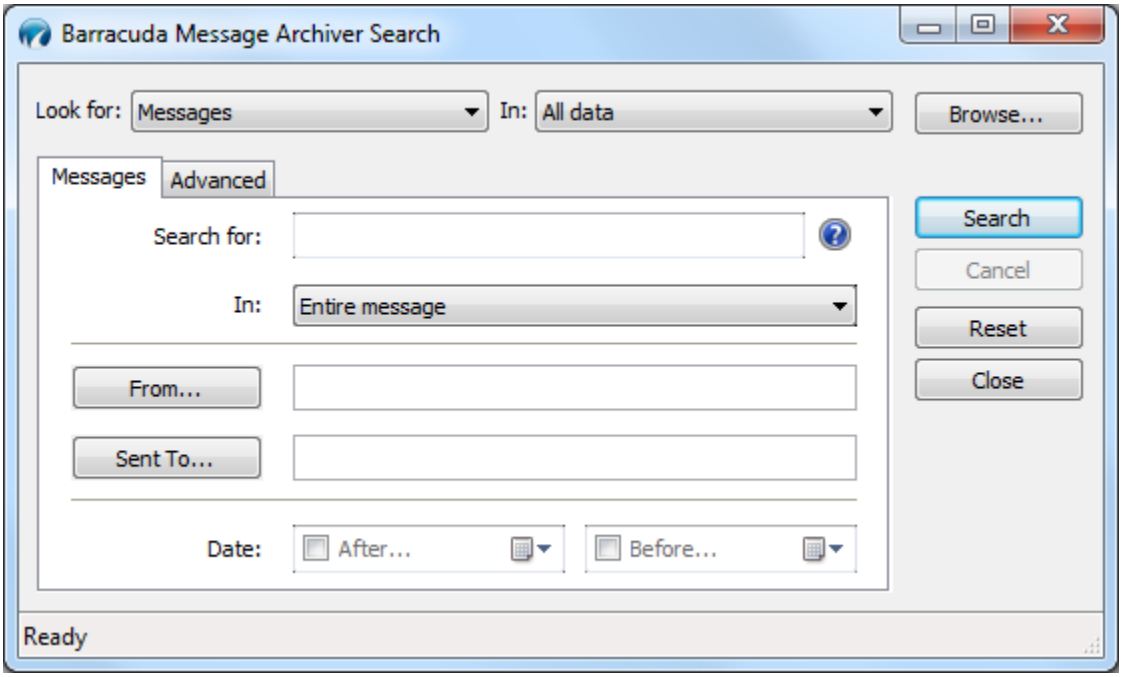
Related Articles

- Installing and Configuring
- Deployment
- Troubleshooting
- Mobile Application for iPhone, iPod Touch, and iPad
- Mobile Application for Android

Microsoft Office Click-to-Run for Office 2010
If you are running Microsoft Office Click-to-Run for Office 2010, Microsoft has reported that the environment has potential issues when running Add-Ins such as the Barracuda Message Archiver Outlook Add-In. As a result, the Barracuda Message Archiver Outlook Add-In may not function as expected. For additional information, refer to the Microsoft Knowledgebase article Office 2010 Click-to-Run compatibility with add-ins.

Searching

To search archived items, click the **Search Archive** ( ) icon to open the **Barracuda Message Archiver Search** dialog box:



- **Look for** drop-down menu - Select the type of item you wish to search for; select **Any type of Item**, **Appointments**, **Contacts**, **Messages**, **Notes**, or **Tasks**.

- **In** drop-down list - Select the search location:
  - **All data** - Search everywhere in the selected item type
  - **Specific folders** - Click **Specific folders**, or click **Browse** to select one or more folders across all of your Archiver stores in which to search; click **OK** to save your selections

> **Release 3.5 and Higher**
>
> In release 3.5 and higher, the administrator can associate an LDAP user or group to a role and list of email addresses in the **USERS > LDAP User Add/Update** page. If addresses are excluded, and a configured user runs a search through the Outlook Add-In, the following whitelist/blacklist rules apply:
>
> - If an address is excluded (blacklisted), the address does not display unless the mail includes the user performing the search to assure that a user can always see their own mail.
> - The exclusion rules always take precedence; addresses that are whitelisted are searchable only if the exclusion rules do not block the mail.
> - If a user is not configured and is a member of a group, then the blacklist/whitelist rules assigned to that group apply to that user.
> - If a user is assigned to a group, when the user logs in via the Outlook Add-In or Barracuda Message Archiver Mobile Application, only that user's mail displays. For example, if an LDAP user has the Auditor role, mail available to the Auditor role does not display.

Search Criteria

The available search criteria differs based on the selected searched item type.

Table 1. Search Criteria.

Search Item Type	Criteria	Description
Any Type of Item Appointments Contacts Messages Notes Tasks	Search for	List of keywords on which to search. If multiple keywords are entered, only items with all of the specified keywords are returned. If keywords are enclosed in double quotes (" "), then only items that contain all of the keywords exactly as specified appear in search results.
	In	The part of the item in which to search for the specified keywords. Options vary based on the selected item.
Appointments	Organized By	Appointment creator. Only those items *organized by* the specified user(s) are searched. Enter user names or email addresses, or click **From** to select users from an address book.
	Attendees	Appointment recipient(s). Only those items that were *sent to* the specified user(s) are searched. Enter user names or email addresses, or click **From** to select users from an address book.
	Date	Date restrictions on the item. Search through only those appointments that were scheduled *after* and/or *before* the specified date(s).
Contacts	Email	Message recipient(s). Only those messages *sent to* or *copied to* the specified user(s) are searched. Enter user names or email addresses, or click **Email** to select users from an address book.

Messages	From	Message sender(s). Only those messages that were *sent from* the specified user(s) are searched. You can enter user names or email addresses, or click **From** to select users from an address book.
	Sent To	Message recipient(s). Only those messages that were *sent to* or *copied to* the specified user(s) are searched. Enter user names or email addresses, or click **Sent To** to select users from an address book.
	Date	Date restrictions on the item. Only those messages that were sent for *after* and/or *bef ore* the specified date(s) are included in the search.
Tasks	Status	Only tasks matching the selected status are searched for the specified text.
	Due	Date restrictions on the tasks. Only those tasks due *after* and/or *before* the specified date(s) are included in the search.

You must specify at least one search criteria from Table 1 to complete a search; if you specify multiple criteria, only messages that meet *all* criteria are returned.

Keywords must be alpha-numeric characters, and are not case sensitive. Additionally, you can use wildcards to represent one or more other characters to use search patterns.

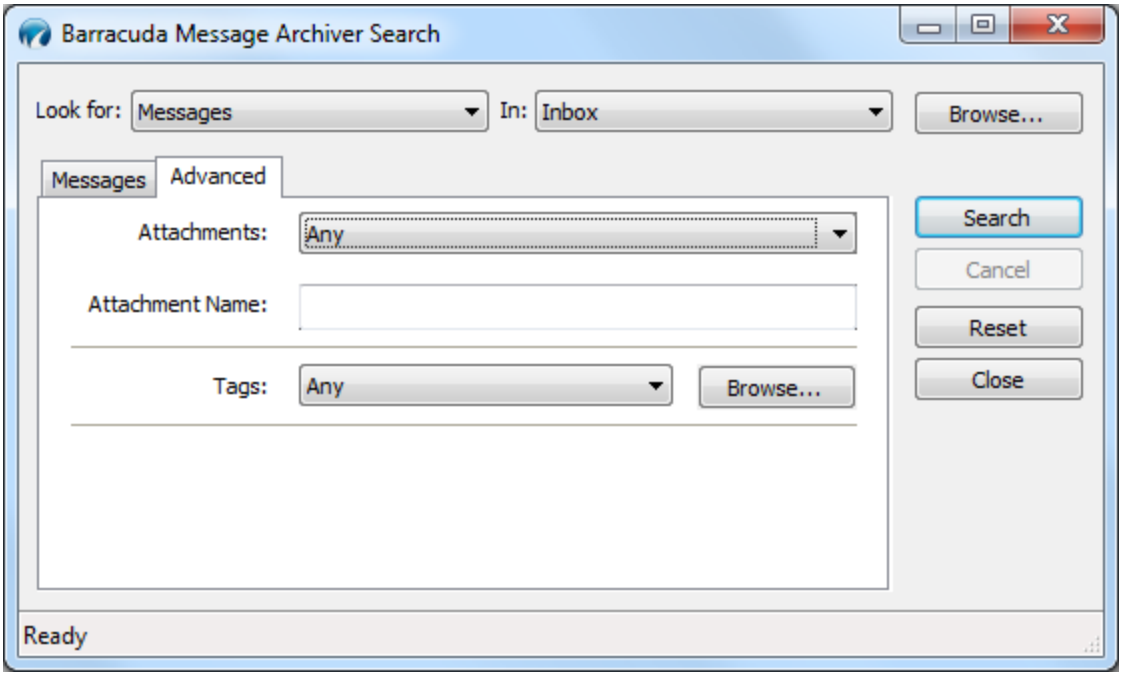
Table 2. Keywords.

Wildcard Symbol	Represents
? (single question mark)	Specifies a single alphanumeric character. Question marks can be appended to search for a specific number of characters, for example, a???a returns five letter words that starts and ends with "a" or "A".
* (asterisk)	Specifies zero or more alphanumeric characters. For example, pl* returns "plane", "planning", etc.

The first character of a keyword *cannot* be a wildcard, and wildcards *cannot* be used when searching for a quote phrase.

Advanced Search Criteria

Click the **Advanced** tab in the **Barracuda Message Archiver Search** dialog box to specify additional search criteria based on attachments and tags:



Any search criteria specified in the **Advanced** tab is used in conjunction with the criteria specified in the selected search item type search tab. Keywords in the **Advanced** tab must be alpha-numeric characters, and are not case sensitive. You can include wildcards in the **Attachment Name** field (refer to Table 3 below for more information).

Table 3. Advanced Search Criteria.

Criteria	Description
Attachments	Number of attachments required in the messages in which to search. Options are *Any, One or more,* or *None*.
Attachment Name	Name of the attachment for which to search. Only messages containing an attachment with the specified name are returned.
Tags	Tag(s) on which to search. *Wildcards are NOT accepted in this field.* Tags are defined and set on messages in the Barracuda Message Archiver web interface. If tags are defined and set on messages, you can use these tags in this field to quickly locate the messages. Options are Any or Specific tags. Contact your system administrator for more information.

Message Results

All messages that match the specified criteria are returned in the search window. Double-click an item to open it in Outlook, or right-click to select an action to perform on the selected item.

Table 4. Available Actions.

Action	Description
Open	Open the selected item in the standard Outlook view; double-clicking an item performs the same action. Once an item is opened, it can be treated as any other non-archived item, including replying to and forwarding.

Reply Reply to All	Creates a *Reply* or *Reply All* to the selected item in the exact same manner as Outlook.
Forward	Crates a *Forward* of the selected item in the exact same manner as Outlook.
Copy to Folder	Opens the **Select Folder** dialog box in Outlook from which you can select a folder to which to copy the selected item(s). Use Ctrl- or Shift-click to select and copy multiple messages in the returned search window to a folder. Select from your existing folders, or create a new folder for the selected item(s). **Important** If the Outlook window is hidden or in the background, you may need to click on the Windows taskbar and bring Outlook to the foreground to complete this action.

Archiving Messages

The Barracuda Message Archiver Outlook Add-in tool includes an option to immediately archive a selected item(s) to the Barracuda Message Archiver. Additionally, if the **Automatically stub attachments when archiving** option is turned on, and you click the **Archive Attachments** (Archive Data) icon:

- A copy of the complete selected item(s) is stored on the Barracuda Message Archiver
- On your mail server, any message attachments that are in the body of an original message(s) are replaced with references to the archived attachment on the Barracuda Message Archiver

This process is known as "attachment stubbing" and helps to reduce the size of both your personal inbox and mail server storage.

To archive a message,

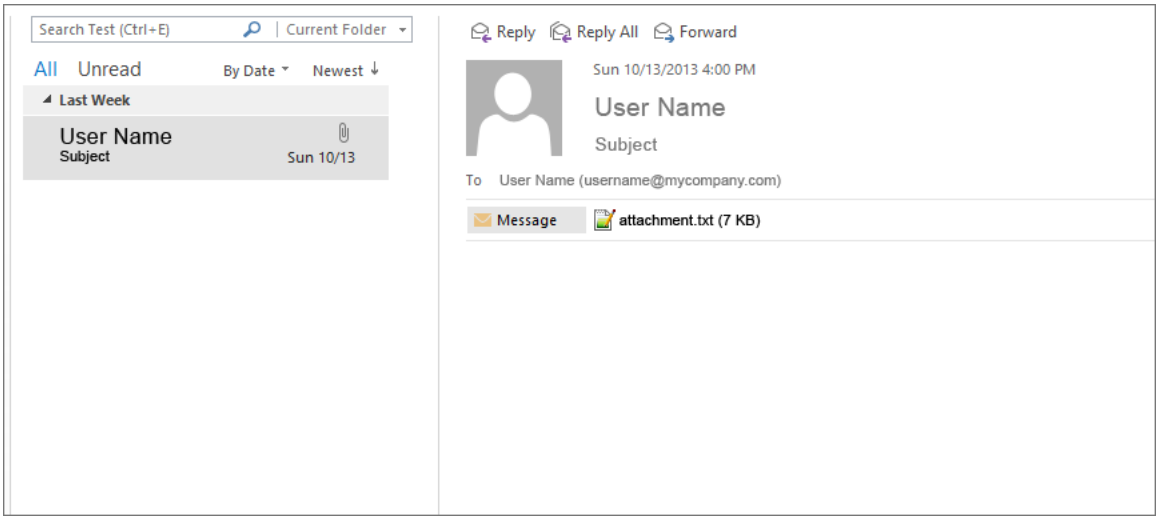
1. Select the desired item(s) in Outlook, and click the **Archive Attachments** (Archive Data) icon; a progress window displays while the item(s) are archived
2. Once the item(s) are successfully archived, any message attachments display as hyperlinks in the Outlook message preview. Click on a hyperlink to view the attachment.
3. Double-click the archived message to open it in the message view; attachments display with icons as they normally would in Outlook.
4. When you click the attachment hyperlink or double-click the archived message, the attachment is retrieved form the Barracuda Message Archiver, allowing you to view or save it in the same manner as an attachment in any other message.

- Using this feature immediately sends the message for archiving; however, if the Barracuda Message Archiver is currently in the midst of archiving other messages, it may be a matter of minutes or even hours before the archived attachments are available. Once archived, the message appears in the Barracuda Message Archiver Outlook Add-in search results.
- Forwarding an archived message automatically includes any attachments in that message as part of the forwarded message. However, a reply to such a message does not automatically include attachments, and the original archived message remains stubbed.

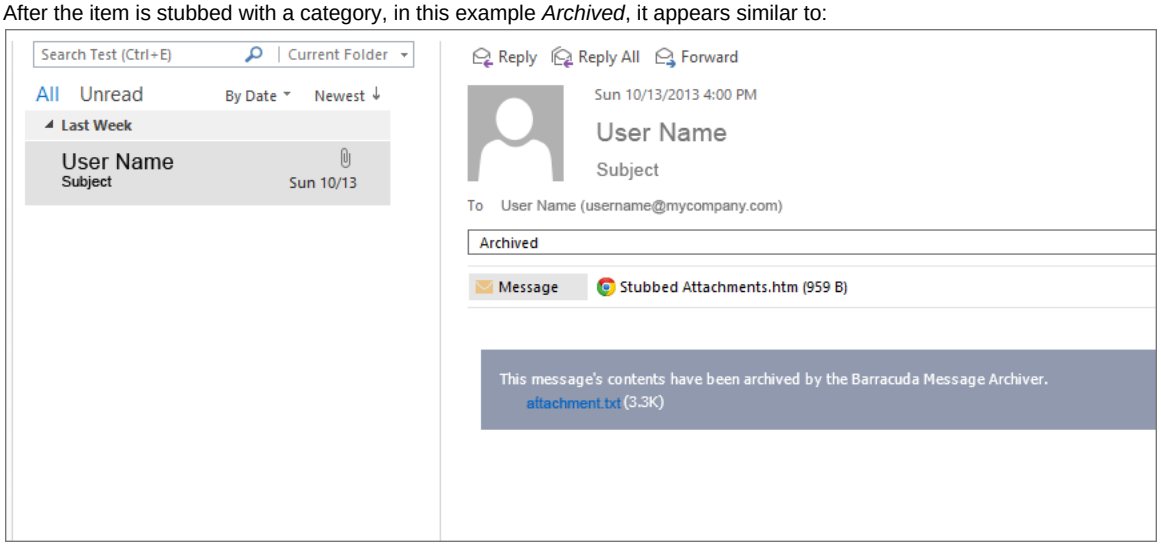
Applying a Category to Archived Items

Firmware Version
This feature is available only in the Barracuda Message Archiver Outlook Add-In version 3.5 and higher.

If enabled by your administrator, a category is applied to all mail archived from the Outlook Add-In. For example, before archival, an item displays

similar to: 

After the item is stubbed with a category, in this example *Archived*, it appears similar to:



Restoring Stubbed Content to Microsoft Exchange

> **Firmware Version**
> This feature is available only in the Barracuda Message Archiver Outlook Add-In version 3.2.30 and higher.

To restore stubbed content to your Microsoft Exchange Server, click the **Restore** (Restore) icon in the Outlook toolbar. When clicked, the selected stub content is restored to the Exchange Server and persists on the Server for 30 days.

> **Installation and Configuration**
> For attachment and whole-message stubbing options, refer to Installing and Configuring the Barracuda Message Archiver Outlook Add-In.

Troubleshooting the Barracuda Message Archiver Outlook Add-In

This article refers to the Barracuda Message Archiver release 3.1 or higher, and the Barracuda Message Archiver Outlook Add-In version 3.1 or higher, except where noted.

Verify the Outlook Add-In version (available for download on the **USERS > Client Downloads** page) is the *same major revision* as the Barracuda Message Archiver firmware for proper functionality.

In this article:

- Components Error
- Unexpected Search Results
- Redirect Failure
- Capturing Log Files

Components Error

> **Microsoft Office Click-to-Run for Office 2010**
> If you are running Microsoft Office Click-to-Run for Office 2010, Microsoft has reported that the environment has potential issues when running Add-Ins such as the Barracuda Message Archiver Outlook Add-In. As a result, the Barracuda Message Archiver Outlook Add-In may not function as expected. For additional information, refer to the Microsoft Knowledgebase article Office 2010 Click-to-Run compatibility with add-ins.

If required Outlook components are missing or incorrectly installed, you may encounter the error **Unable to initialize required components** whe n performing some operations in the Barracuda Message Archiver Outlook Add-In.

To resolve this error, complete the following steps.

1. Use the steps outlined on the Microsoft Knowledgebase to repair your installation of Microsoft Outlook:
   - Microsoft Office 2003: http://support.microsoft.com/kb/821593
   - Microsoft Office 2007: http://support.microsoft.com/kb/924611
   - Microsoft Office 2010: http://office.microsoft.com/en-us/project-help/repair-or-remove-office-HA010357402.aspx

   > **Test**
   > Restart Outlook and attempt the operation that originally initiated the error message. If the operation is successful, no further steps are necessary, however, if the problem persists, complete **Step 2**.
2. Verify that you have not installed Microsoft Office components from different versions of Microsoft Office, for example, Microsoft Outlook 2007 and Microsoft Word 2010. If you determine that different versions are installed, uninstall the Microsoft Office components, and then reinstall using only the Microsoft Office components that correspond with the *desired version of Microsoft Outlook*.

   > **Test**
   > Restart Outlook and attempt the operation that originally initiated the error message. If the operation is successful, no further steps are necessary, however, if the problem persists, complete **Step 3**.
3. Use the steps outlined on the Microsoft Knowledgebase to install the Microsoft Office Primary Interop Assemblies:
   - Microsoft Office 2003: http://www.microsoft.com/en-us/download/details.aspx?id=20923
   - Microsoft Office 2007: http://www.microsoft.com/en-us/download/details.aspx?id=18346
   - Microsoft Office 2010: http://www.microsoft.com/en-us/download/details.aspx?id=3508

   > **Test**
   > Restart Outlook and attempt the operation that originally initiated the error message. If the operation is successful, no further steps are necessary, however, if the problem persists, complete step 4.
4. Completely uninstall Microsoft Outlook, restart your computer, and reinstall Microsoft Outlook.

   > **Test**
   > Restart Outlook and attempt the operation that originally initiated the error message. If the operation is successful, no further steps are necessary, however, if the problem persists, contact Barracuda Networks Technical Support for further assistance.

Unexpected Search Results

In release 3.5 and higher, the administrator can associate an LDAP user or group to a role and list of email addresses in the **USERS > LDAP User Add/Update** page. If addresses are excluded, and a configured user runs a search through the Outlook Add-In, the following whitelist/blacklist rules apply:

- If an address is excluded (blacklisted), the address does not display unless the mail includes the user performing the search to assure

that a user can always see their own mail.
- The exclusion rules always take precedence; addresses that are whitelisted are searchable only if the exclusion rules do not block the mail.
- If a user is not configured and is a member of a group, then the blacklist/whitelist rules assigned to that group apply to that user.
- If a user is assigned to a group, when the user logs in via the Outlook Add-In or Barracuda Message Archiver Mobile Application, only that user's mail displays. For example, if an LDAP user has the Auditor role, mail available to the Auditor role does not display.

Contact your Barracuda Message Archiver administrator for exclusion rules.

Redirect Failure

In firmware release 3.5 and higher and Barracuda Message Archiver Outlook Add-In version 3.5 and higher, the Outlook Add-In requires secure (HTTPS) connectivity to the Barracuda Message Archiver. If an insecure (HTTP) connection is attempted the Outlook Add-In is redirected to use *https:* with the configured secure port (the default port is 443). If users encounter a redirect failure, verify the following:

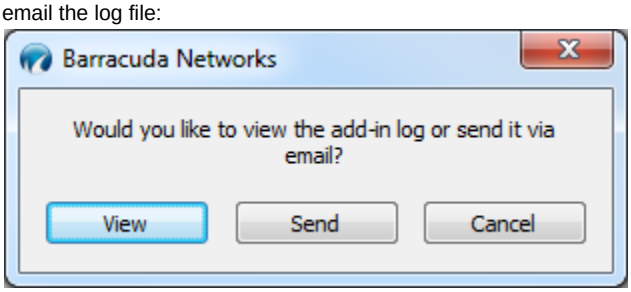
- The URI uses HTTPS and *not* HTTP
- The network firewall rules have been updated to allow connectivity to complete on the secure port

See Installing and Configuring the Barracuda Message Archiver Outlook Add-In for details on updating the URI.

Capturing Log Files

If requested to do so by Barracuda Networks Technical Support, use the following steps to capture the Outlook Add-In log files based on the version of Microsoft Office Outlook.

- Microsoft Office 2003 and 2007: In Outlook, go to **Tools > Options > Barracuda > Barracuda Message Archiver Add-In**, and then double-click on the version number.
- Microsoft Office 2010 and newer: In Outlook, go to **File > Barracuda Networks**, click **View Log**, and then specify whether to view or email the log file:



How to Enable the Barracuda Message Archiver Outlook Add-In in a Microsoft Terminal Server Environment

This section refers to Barracuda Message Archiver firmware release 3.1 and higher, the Barracuda Outlook Add-In release 3.1 and higher, and Microsoft Outlook 2003 and 2007, except where noted.

Verify the Outlook Add-In version (available for download on the **USERS > Client Downloads** page) is the *same major revision* as the Barracuda Message Archiver firmware.

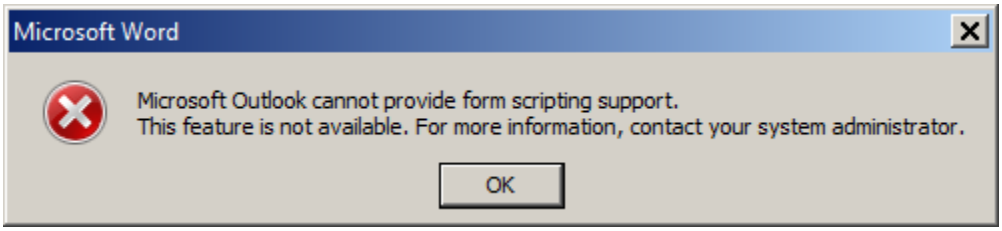
In this article:

- Method 1: Copy the Outlvbs.dll File to Existing Installations
- Method 2: Custom Installation Wizard

Related Articles
• Search and Archive • Troubleshooting

Additional Resource
• Forms with VBScript do not work with Terminal Services in Outlook • Barracuda Networks Knowledgebase Solution #00 006099

By default Microsoft Office 2003 and Office 2007 do not install the VBScript component in windows Terminal Server environments. For this reason, if you are running a copy of Outlook 2003 or 2007 in a Windows Terminal Server with remote users connecting to the server to run Outlook, users may encounter an error similar to the following when using the Barracuda Outlook Add-In with Outlook 2003 or 2007 running in this environment:


Microsoft Word
Microsoft Outlook cannot provide form scripting support.
This feature is not available. For more information, contact your system administrator.
OK

Contact your Terminal Services Administrator for more information on your organization's set up. For additional information, refer to the Microsoft Support article **Forms with VBScript do not work with Terminal Services in Outlook**.

Use one of the following methods to work around this issue and to enable the Barracuda Outlook Add-In:

- Method 1: Copy the Outlvbs.dll File to Existing Installations
- Method 2: Custom Installation Wizard

Method 1: Copy the Outlvbs.dll File to Existing Installations

Click here to expand...

Use the following steps to copy the **Outlvbs.dll** file to existing installations:

1. Log onto a computer that is running a full, standalone version of Microsoft Office.
2. Copy the file **Outlvbs.dll** from the folder:
    - For Microsoft Office 2003, copy the file from **Program Files\Microsoft Office\Office11**.
    - For Microsoft Office 2007, copy the file from **Program Files\Microsoft Office\Office12** .
3. Log onto a computer that is running Microsoft Outlook from the Terminal Server, and is encountering the form scripting error.
4. Paste the file **Outlvbs.dll** from step 2 to the folder:
    - For Microsoft Office 2003, paste the file into the folder **Program Files\Microsoft Office\Office11**.
    - For Microsoft Office 2007, paste the file into the folder **Program Files\Microsoft Office\Office12**.

If the Terminal Server is running Microsoft Office 2010, copy the **Outlvbs.dll** file to the **Program Files\Microsoft Office\Office14** f older.

Method 2: Custom Installation Wizard

Click here to expand...

Use the following steps to use the Custom Installation Wizard to deploy Microsoft Office with an additional property to let the VBScript component to be installed.

For Microsoft Office Outlook 2003:

1. Log onto the Microsoft Terminal Server, and open the Custom Installation Wizard.
2. Create a new Installer transform **(MST)** file for the Microsoft Office installation.
3. Configure your installation requirement in the Custom Installation Wizard.
4. On page 23 of 24 of the Custom Installation Wizard, click **Modify Setup Properties**, and click **Add** and enter the following property name and value: **Property Name: WTSDISABLED Value: MsInfoFiles,PPTCastCoreFiles**

Both the property name and the value are case sensitive.

5. Complete the Custom Installation Wizard.

For Microsoft Office Outlook 2007:

1. Log onto the Microsoft Terminal Server, and Install Microsoft Outlook 2007 as a standalone application or as part of a 2007 Office suite.
2. Determine the globally unique identifier (GUID) for the product that you installed in Step 1. If you installed Outlook, use that product GUID. If you installed Office Enterprise 2007, use that product GUID.

   For more information about how to determine the installed product GUID, refer to the Microsoft knowledgebase solution De scription of the numbering scheme for product code GUIDs in 2007 Office suites and programs.

3. After you have the product GUID, at a command line, run the following command:

   `msiexec /i <Product Code GUID of [SKUName]WW.msi> ADDLOCAL=OutlookVBScript /qb`

   In this command, replace `<Product Code GUID of [SKUName]WW.msi>` with your product GUID.

   For example, if you have Office Enterprise 2007 installed, your product GUID would be the following: `{90120000-0030-0000-0000-0000000FF1CE}`

   Therefore, the command line should appear as follows: `msiexec /i {90120000-0030-0000-0000-0000000FF1CE} ADDLOCAL=OutlookVBScript`

Barracuda Outlook Add-In Customization Options

This article refers to the Barracuda Message Archiver release 3.1 or higher, and the Barracuda Outlook Add-In Deployment Kit 3.1 or higher, except where noted.

The Barracuda Outlook Add-In Deployment Kit is available for download from the **USERS > Client Downloads** page in the Barracuda Message Archiver web interface. Additionally from this page, verify the Outlook Add-In version is the *same major revision* as the Barracuda Message Archiver firmware.

This Barracuda Outlook Add-In Deployment Kit includes an administrative template that allows you to enforce or modify certain functionality and features included in the Barracuda Outlook Add-In. You can use this template to customize your deployment.

Additional Resource

- Recognized Environment Variables

The following table describes the customizable features:

Feature	Description
General	

Barracuda Message Archiver URL	Complete URL (e.g., `https://archiver.mycompany.com:443`) Microsoft® Outlook® users use to connect to the Barracuda Message Archiver. • URL must be externally accessible if users plan to access the Barracuda Message Archiver outside your local network • Using HTTPS is recommended • Append the URL with the Barracuda Message Archiver port number, for example `:443` • You do not need to specify the default HTTPS port 443 • To prohibit users from specifying a different URL, turn on **Require Users to Use Configured URL**
Hide Toolbar Elements	Specify the toolbar elements you want to hide: • **Hide All Toolbar Buttons** - No archiving or search actions are available to users • **Hide Only Archiving Buttons** - Users can search, but cannot archive or stub messages • **Hide Only Search Buttons** - Users can archive and stub messages, but cannot search • **Hide Only Archiver Store Buttons** - Users cannot see their Archiver stores (mailboxes) These settings do not affect the ability to use the custom form installed by the Barracuda Outlook Add-In for viewing, forwarding, or replying to stubbed messages. The settings here affect both the Explorer and Inspector views in Outlook.
Hide Outlook Options Page	When turned on, users cannot modify their Barracuda Outlook Add-In configuration.
Search	
Message Copy Limit	Specify the maximum number of messages in a single operation that a user can copy from the integrated Outlook search to reduce Excessive message copying from the Barracuda Message Archiver to either a Microsoft Exchange account or to a PST file can be resource-intensive. Set this limit low to discourage users from copying a large number of messages in a single session. Instead, users can copy messages in multiple copy operations. Set this value to '0' to disable all message copying.
Maximum Cache Size	Specify the maximum search cache size in megabytes (MB).
Search Cache Path	Specify the search cache path; this path can include environment variables[(1)]. If the path is not set, the default path is set to: `%USERPROFILE%\AppData\Local\Barracuda\Message Archiver\Outlook Add-In\Cache`
Coerce All HTML Message Bodies to UTF-8 when Displaying	When enabled, the Barracuda Add-In converts all message HTML bodies to UTF-8 when displayed in Outlook. ⚠ **Important - Barracuda Networks Technical Support** Enable this feature *only* if you have been advised to do so by Barracuda Networks Technical Support.

Archiving (firmware release 3.5 and higher only)	
Stub Entire Message	Specify whether to stub the entire message.
Category to Apply to Archived Items	Specify whether to apply a category to items archived or stubbed by the Barracuda Outlook Add-In. When enabled, enter the category name in the **Category** field, for example, enter **Stored**.
Stub Caching	
Disable Stub Caching	Specify whether users can cache stubbed messages for offline access.
Maximum Cache Size	Specify the maximum stub cache size in MB.
Maximum Message Age	Specify the maximum number of days cached messages are stored.
Stub Cache Path	Specify the stubbed message cache path; this path can include environment variables[(1)].
Archiver Store	
Disable Archiver Stores	Specify whether to disable Archiver stores. When turned on, the user cannot create or synchronize Archiver stores (mailboxes), and all relevant UI elements are hidden or disabled.
Disable Sync if Exchange Mailbox Stores	Specify whether users can synchronize Exchange mailbox stores from the Barracuda Message Archiver. When turned on, users can synchronize PST files only.
Maximum Message Age	Specify the maximum number of days users can select when synchronizing Exchange mailbox stores.
Maximum Disk Usage	Specify the maximum disk usage in MB available for Archiver stores. When enabled, users cannot add new Archiver stores that exceed the specified usage limit. If the usage limit is reached, existing store are not synchronized.
Location of New Archiver Stores	Specify the directory path where new Archiver stores are to be created. This path can include environment variables[(1)]. If the path is not set, the default path is set to: `%USERPROFILE%\AppData\Local\Barracuda\Message Archiver\Outlook Add-In\stores`
Sync Schedule	Specify the daily Archiver store sync time. By default, synchronization runs between 4:00am and 6:00 am. • **Sync Start Time** - Start time must be between 0 (midnight) and 23 (11:00pm) • **Sync Window** - Number of hours after the **Sync Start Time** valu e that the sync can begin; use this to avoid consuming too many Archiver resources during multi-client simultaneous synchronization. The system must be powered on and the user must be logged in for the scheduled synchronization to be performed, otherwise the synchronization is performed upon user log in.

Notes:

[(1)] For more information on environment variables, refer to the Microsoft technet article Recognized Environment Variables.

How to Create Local Mailstores

This article refers to the Barracuda Message Archiver release 3.1 or higher, and the Barracuda Message Archiver Outlook Add-In version 3.1 or higher, and Microsoft Outlook 2003, 2007, or 2010.

In this article:

- Outlook 2003, 2007, and 2010
- Enable Scripting Organization-Wide (Recommended)
- Enable Scripts on User Systems
  - Enable Scripts in Microsoft Outlook 2003
  - Enable Scripts in Microsoft Outlook 2007
  - Enable Scripts in Microsoft Outlook 2010

Related Articles

- Barracuda Message Archiver Outlook Add-In Deployment

Configuration Guidelines
This article is intended as a configuration *guideline*; your deployment will be specific to your environment. Any administrative changes should be reviewed with your IT team before proceeding.

Outlook 2003, 2007, and 2010

By default in Microsoft Outlook 2003, 2007, and 2010, a security setting does not allow script execution or custom forms in shared mailboxes or public folders. For this reason, if the Microsoft Exchange Administrator performs message stubbing on shared mailboxes or public folders delegated to all users or specific user groups, these stubbed messages cannot be retrieved in the Barracuda Message Archiver Outlook Add-In. To allow users to retrieve these stubbed messages in addition to their **Inbox** messages, each user can set **Allow Script in shared folders**, or the Microsoft Exchange Administrator can enable scripts in folders organization-wide using the Microsoft Office policy template (ADM) files.

Microsoft Outlook 2013
In Microsoft Outlook 2013, script execution is allowed by default.

Enable Scripting Organization-Wide (Recommended)

To enable scripts across your entire organization, go to the associated Microsoft article:

- Microsoft Outlook 2003 - See the Microsoft article Office 2003 Service Pack 3 Administrative Template (ADM) OPAs, and Explain Text Update, verify your operating system in the section ***System requirements***, and following the steps described in the section ***Instructions***.
- Microsoft Outlook 2007 - See the Microsoft article 2007 Office system Administrative Template files (ADM, ADMX, ADML) and Office Customization Tool version 2.0, your operating system in the section ***System requirements***, and following the steps described in the section ***Instructions***.
- Microsoft Outlook 2003 - See the Microsoft article Office 2010 Administrative Template files (ADM, ADMX/ADML) and Office Customization Tool download, verify your operating system in the section ***System requirements***, and following the steps described in the section ***Instructions***.

Once you download and set up the ADM template files, open the associated Outlook ADM file:

- For Outlook 2003, open the ADM file **outlk11.adm**
- For Outlook 2007, open the ADM file **outlk12.adm**
- For Outlook 2010, open the ADM file **outlk14.adm**

In the ADM file, set `VALUEON NUMERIC` to '`1`' and `VALUEOFF NUMERIC` to '`0`' for the following values:

- `VALUENAME SharedFolderScript`
- `VALUENAME PublicFolderScript`

For example, update the ADM file **outlk11.adm** to display as:

```
POLICY "Disable scripts for shared folders"

KEYNAME Software\Policies\Microsoft\Office\11.0\Outlook\Security
        PART "Check to disable scripts for shared folders" CHECKBOX
                                VALUENAME SharedFolderScript
                                VALUEON NUMERIC 1 DEFCHECKED
                                VALUEOFF NUMERIC 0
        END PART
        END POLICY
POLICY "Disable scripts for public folders"
KEYNAME Software\Policies\Microsoft\Office\11.0\Outlook\Security
        PART "Check to disable scripts for public folders" CHECKBOX
                                VALUENAME PublicFolderScript
                                VALUEON NUMERIC 1
                                VALUEOFF NUMERIC 0
        END PART
        END POLICY
```

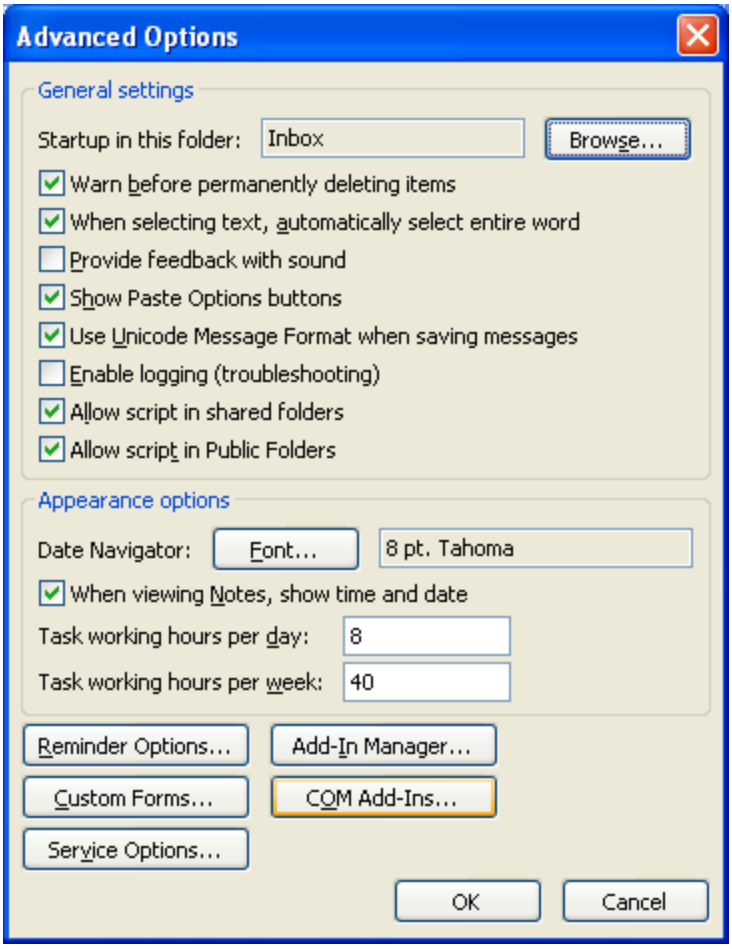
Enable Scripts on User Systems

If you do not wish to use ADM templates to allow scripting across the entire organization, you can direct each user to enable scripts for shared and public folders based on their installed version of Microsoft Outlook.

Enable Scripts in Microsoft Outlook 2003

Use the following steps to enable scripts in shared and public folders in Outlook 2003:

1. Log into Microsoft Outlook 2003.
2. On the **Tools** menu, click **Options**.
3. In the **Options** dialog box, click the **Other** tab, and click **Advanced Options**.
4. In the **General Settings** pane, turn on **Allow Script in shared folders** and **Allow script in Public Folders:**

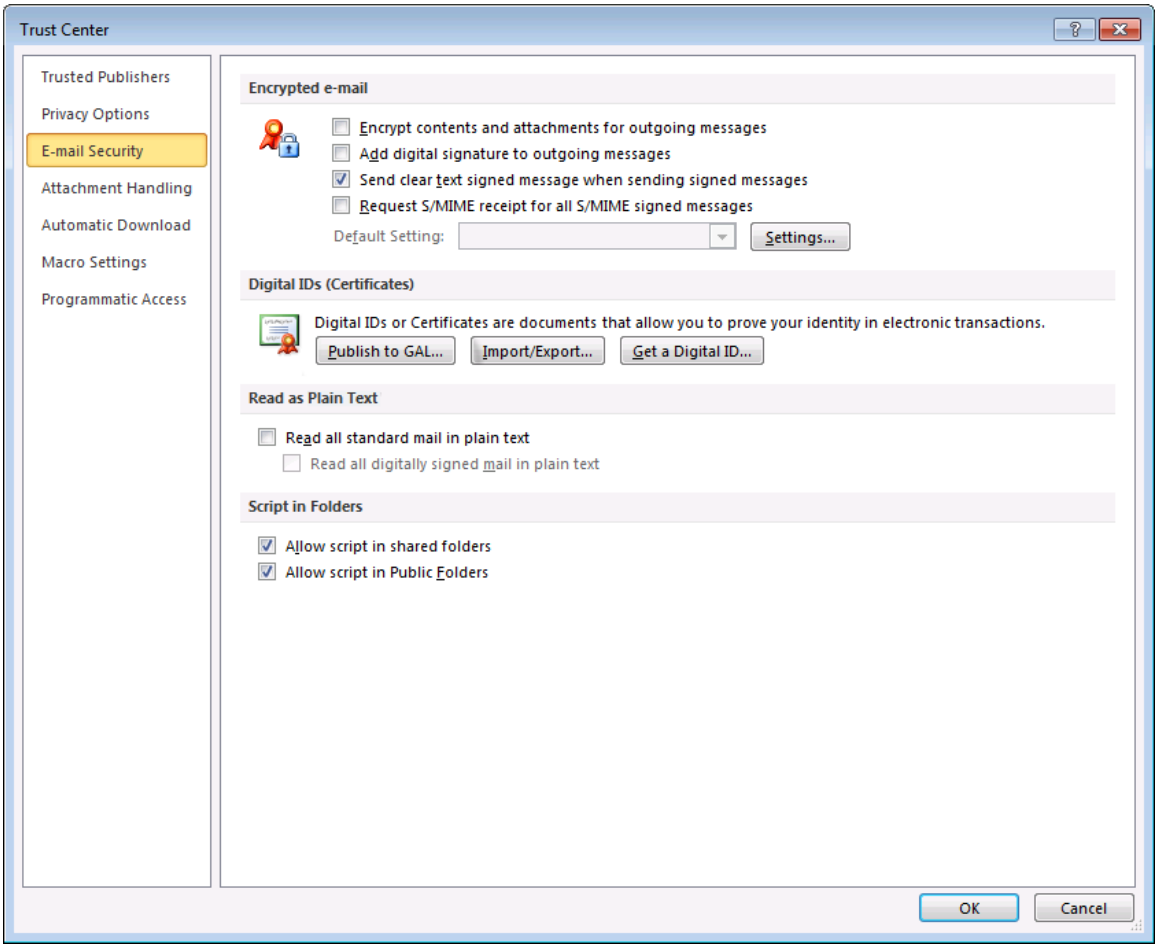


5. Click **OK** to save your settings.

Enable Scripts in Microsoft Outlook 2007

Use the following steps to enable scripts in shared and public folders in Outlook 2007:

1. Log into Microsoft Outlook 2007.
2. On the **Tools** menu, click **Trust Center**.
3. In the Navigation Pane, click **E-mail Security**.
4. In the **Script in Folders** section, turn on **Allow script in shared folders** and **Allow script in Public Folders**:

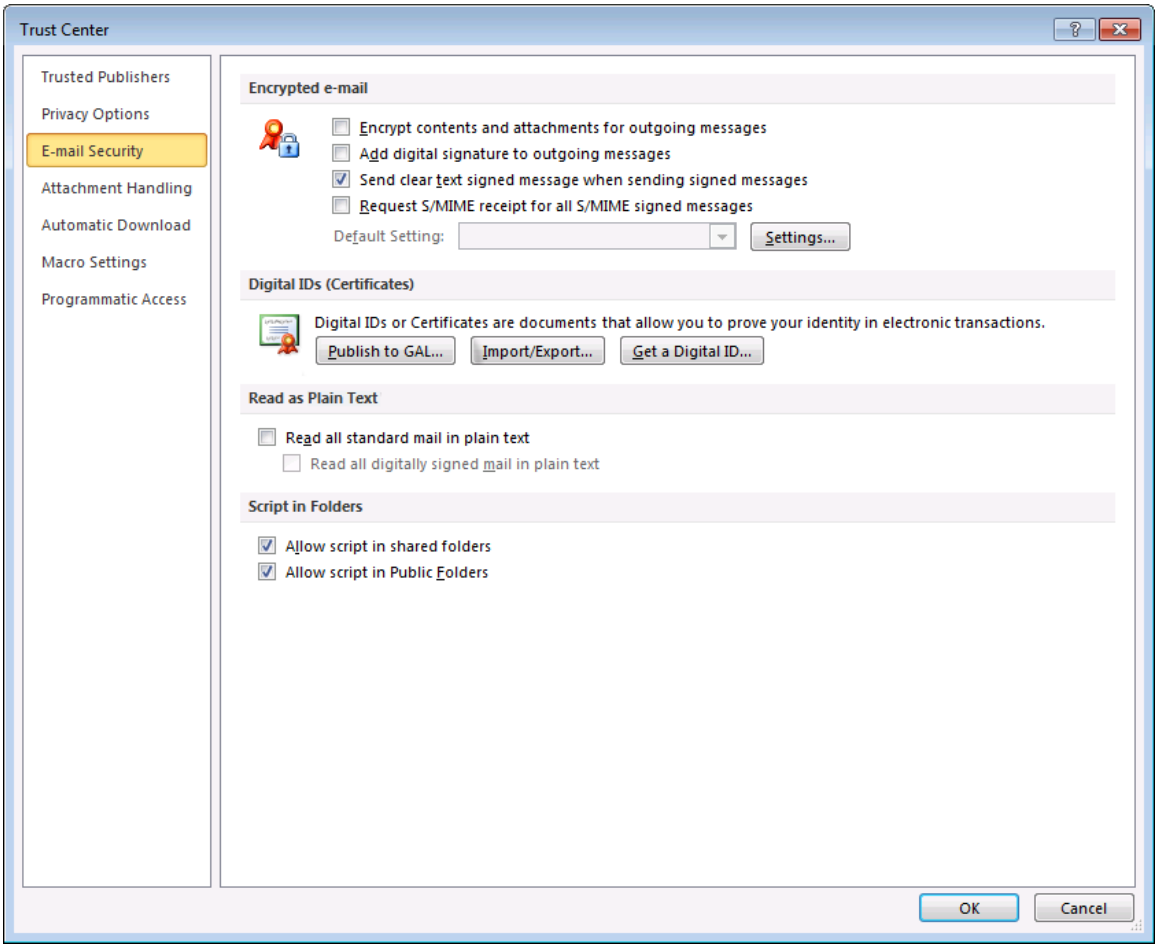

Trust Center
Trusted Publishers
Privacy Options
E-mail Security
Attachment Handling
Automatic Download
Macro Settings
Programmatic Access
Encrypted e-mail
Encrypt contents and attachments for outgoing messages
Add digital signature to outgoing messages
Send clear text signed message when sending signed messages
Request S/MIME receipt for all S/MIME signed messages
Default Setting:
Settings...
Digital IDs (Certificates)
Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.
Publish to GAL...
Import/Export...
Get a Digital ID...
Read as Plain Text
Read all standard mail in plain text
Read all digitally signed mail in plain text
Script in Folders
Allow script in shared folders
Allow script in Public Folders
OK
Cancel

5. Click **OK** to save your settings.

Enable Scripts in Microsoft Outlook 2010

Use the following steps to enable scripts in shared and public folders in Outlook 2010:

1. Log into Microsoft Outlook 2010.
2. On the **File** menu, click **Options**.
3. In the Navigation Pane, click **Trust Center**, and then click **Trust Center Settings**.
4. In the Navigation Pane, click **E-mail Security**, and in the **Script in Folders** section, turn on **Allow script in shared folders** and **Allow script in Public Folders**:


Trust Center
Trusted Publishers
Privacy Options
E-mail Security
Attachment Handling
Automatic Download
Macro Settings
Programmatic Access
Encrypted e-mail
Encrypt contents and attachments for outgoing messages
Add digital signature to outgoing messages
Send clear text signed message when sending signed messages
Request S/MIME receipt for all S/MIME signed messages
Default Setting:
Settings...
Digital IDs (Certificates)
Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.
Publish to GAL...
Import/Export...
Get a Digital ID...
Read as Plain Text
Read all standard mail in plain text
Read all digitally signed mail in plain text
Script in Folders
Allow script in shared folders
Allow script in Public Folders
OK
Cancel

5. Click **OK** to save your settings.

Barracuda Message Archiver Mobile Applications

In This Section

- Barracuda Message Archiver Mobile Application for iPhone, iPod Touch, and iPad
- Barracuda Message Archiver Mobile Application for Android

Barracuda Message Archiver Mobile Application for iPhone, iPod Touch, and iPad

Requirements:

- Barracuda Message Archiver firmware version 3.5 or higher
- Barracuda Message Archiver URI from your system administrator
- Latest iPhone Barracuda Archive Search application available for download from iTunes: https://itunes.apple.com/us/app/barracuda-archive-search/id684270246
- iPhone, iPod Touch, or iPad running iOS 4.3 or later
- Email address archived by your organization's Barracuda Message Archiver
- Barracuda Message Archiver HTTPS port number

In this article:

- Configuration
- Searching for Archived Messages
- Advanced Search Settings
- Message Results
- Replying to and Forwarding Archived Messages

Related Articles
• Install/Configure the Outlook Add-In

Secure Connectivity
The Barracuda Message Archiver Companion mobile application requires secure (HTTPS) connectivity to the Barracuda Message Archiver. If an insecure (HTTP) connection is attempted the mobile application is redirected to use *https:* with the configured secure port.

For existing mobile application users, if your URI was originally set up on an earlier firmware version, verify that the URI uses HTTPS. If the URI was set up using HTTP, use the steps in the section **Configuration** to update the URI. If the URI is *not* updated, users are automatically redirected to the secure, HTTPS protocol. This redirection may require an update to your network firewall rules to allow connectivity to complete on the secure port.

Certificates
When using HTTPS connectivity, if a self-signed or private certificate is in place on the Barracuda Message Archiver, your mobile phone operating system (OS) may require you to accept the private certificate before you can download content with the mobile OS download utility. The mechanism to add a private certificate to your mobile device varies; please consult your manufacturer instructions for more information.

The Barracuda Message Archiver Companion mobile application allows you to perform various actions with your messages that are stored on your organization's Barracuda Message Archiver including:

- Search for archived messages based on email content, or constrain the search to a date range, a specific sender, or subject line content;
- Search deleted messages and emails no longer visible in your mail application;
- View and interact with (reply to, reply all, or forward) archived messages.

These actions are available directly from your iPhone, iPod Touch, or iPad, allowing transparent access to, and interaction with, your archived messages.

Only archived messages are available for search with the Barracuda Message Archiver mobile application; non-email items such as calendar entries and contacts are not included in search results.

Configuration

To search your archived mail from your iPhone or other supported device, you must first enter your organization's Barracuda Message Archiver settings, as well as your email address and password.

Email Password Characters
If your email password contains certain punctuation characters, for example the pound '#' symbol, you may encounter problems searching archived messages on the Barracuda Message Archiver from iPhone Archived Mail.

If you attempt to search archived messages before configuring the settings, an error displays. Enter the following details:

- Barracuda Message Archiver hostname or IP address;
- Barracuda Message Archiver HTTPS port number;
- Your corporate email address from which messages are archived;
- Your email password.

Use the following steps to get started.

1. Before you can set up Archived Mail, you need your Barracuda Message Archiver URI from your system administrator. For example: `https://archiver.company.com:8000`
2. Launch Barracuda Archived Mail, and tap **Settings**; the **Settings** page displays.
3. Tap in the **Host** field, and enter your organization's hostname or IP address. For example, enter: `https://archiver.company.com` or **`192.168.200.200`**
4. Tap in the **Port** field and enter the HTTPS port number. For example, enter `8000`
5. In the **Email** field, tap and enter your email address from which to access archived messages. For example,

enter: `myname@company.com`

6. Tap in the **Password** field, and enter your password for the specified email address.
7. Confirm your settings, and tap **Save** at the top of the screen.

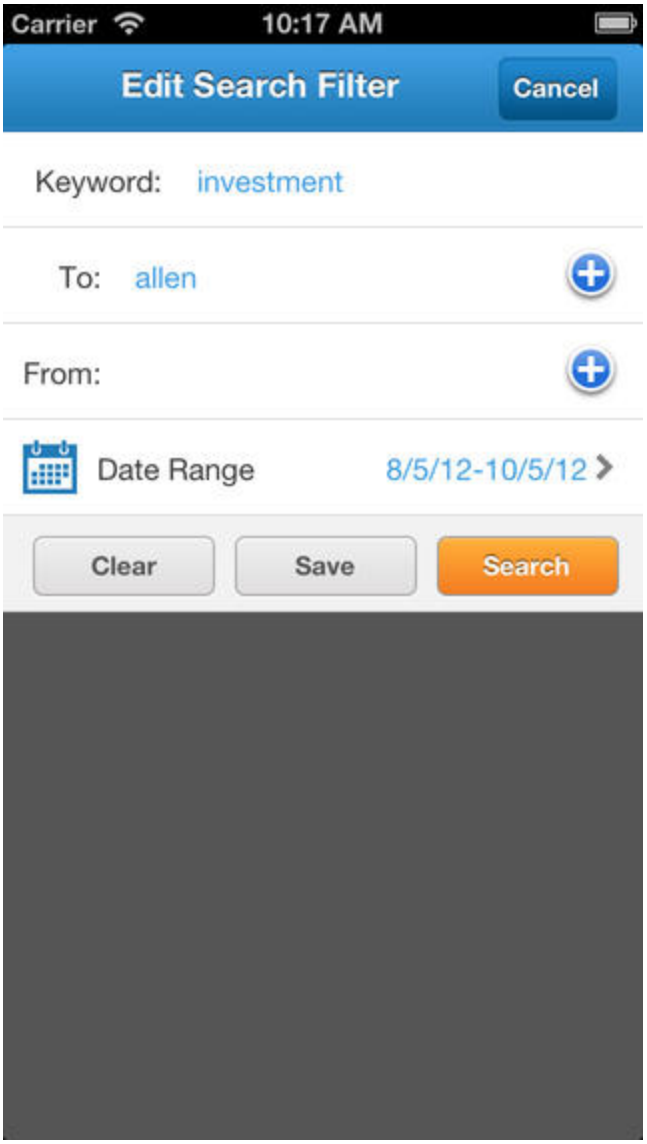
Searching for Archived Messages

Once configuration is complete, you can begin searching your archived emails. Tap **Email** at the top of the view, and tap on the desired search criteria.

> The Barracuda Message Archiver administrator can associate an LDAP user or group to a role and list of email addresses in the **USERS > LDAP User Add/Update** page. If addresses are excluded, and a configured user runs a search through the Barracuda Message Archiver Mobile Application, the following whitelist/blacklist rules apply:
>
> - If an address is excluded (blacklisted), the address does not display unless the mail includes the user performing the search to assure that a user can always see their own mail.
> - The exclusion rules always take precedence; addresses that are whitelisted are searchable only if the exclusion rules do not block the mail.
> - If a user is not configured and is a member of a group, then the blacklist/whitelist rules assigned to that group apply to that user.
> - If a user is assigned to a group, when the user logs in via the Outlook Add-In or Barracuda Message Archiver Mobile Application, only that user's mail displays. For example, if an LDAP user has the Auditor role, mail available to the Auditor role does not display.

Table 1. Search Criteria.

Criteria	Description
All	Returns all messages that contain the search string anywhere in the **From** field, subject line, or email content.
Subject	Returns messages that contain the keyword only in the subject line.
From	Returns messages that contain the keyword only in the **From** field.
Advanced	Restrict the results to a predefined date range. Only those emails sent within the specified date(s) are returned in the search.



Tap in the Search field to display the keypad. Use the keypad to enter the desired keyword or search string; you must enter at least one keyword to perform a search. Keywords must be alpha-numeric characters, and are not case sensitive. Additionally, you can use wildcards to represent one or more other characters to use search patterns.

Table 2. Wildcards.

Wildcard Symbol	Represents
? (single question mark)	Specifies a single alphanumeric character. Question marks can be appended to search for a specific number of characters, for example, a???a returns five letter words that starts and ends with "a" or "A".
* (asterisk)	Specifies zero or more alphanumeric characters. For example, pl* returns "plane", "planning", etc.

Once you specify the keyword and select the search criteria, tap **Search** to display the first 100 messages matching your search criteria, or tap **Cancel** to clear the field and enter a new keyword or search string.

A search is performed on all of your mail folders, including trash and deleted items.

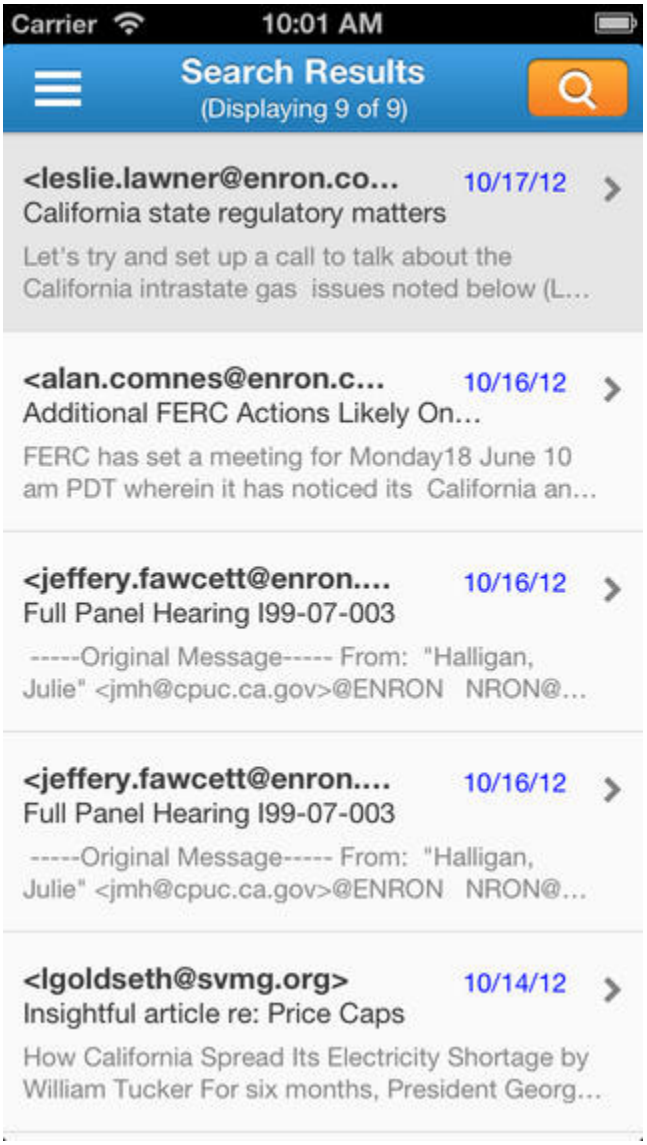
Advanced Search Settings

To specify a specific date range in which to search, tap **Advanced** at the top of the view. The **Advanced Search** page displays the current date. To change the date range, tap on **Date Range**. Tap on the desired date to update the field with your selection.

> The date selected in the **Date To** field must be the *same* or *later* date than the date selected in the **Date From** field.
>
> Any criteria specified in **Advanced** settings is used in conjunction with the criteria specified in the Search field; define your date range, and select **Advanced** from a Search to use the specified date range in conjunction with the keyword to search archived messages.

Message Results

All messages matching the specified criteria display in the search results:


Carrier
10:01 AM
Search Results
(Displaying 9 of 9)
<leslie.lawner@enron.co...
10/17/12
California state regulatory matters
Let's try and set up a call to talk about the California intrastate gas issues noted below (L...
<alan.comnes@enron.c...
10/16/12
Additional FERC Actions Likely On...
FERC has set a meeting for Monday18 June 10 am PDT wherein it has noticed its California an...
<jeffery.fawcett@enron....
10/16/12
Full Panel Hearing I99-07-003
-----Original Message----- From: "Halligan, Julie" <jmh@cpuc.ca.gov>@ENRON NRON@...
<jeffery.fawcett@enron....
10/16/12
Full Panel Hearing I99-07-003
-----Original Message----- From: "Halligan, Julie" <jmh@cpuc.ca.gov>@ENRON NRON@...
<lgoldseth@svmg.org>
10/14/12
Insightful article re: Price Caps
How California Spread Its Electricity Shortage by William Tucker For six months, President Georg...

Replying to and Forwarding Archived Messages

Once you have completed a search of your archived messages, you can view the message, reply to the message, or forward the message.

- Tap on a message to display the full content in the window
- Tap the **Details** (>) icon to the right of a message; a pop-up window displays the available additional actions:
  - **Reply to** - Sends an email response only to the message originator.
  - **Reply all** - Sends an email response to the message originator and all recipients
  - **Forward** - Send a copy of the archived message to one or more new email addresses.
- Tap on an item, or tap the **Details** (>) icon to view the selected message.

Barracuda Message Archiver Mobile Application for Android

Requirements:

- Barracuda Message Archiver firmware version 3.5 or higher
- Barracuda Message Archiver URI from your system administrator
- Latest Android Message Archive application available for download from the Google Play Store: https://play.google.com/store/apps?hl=en
- Android phone or tablet running software version 2.3.3 or greater
- Email address archived by your organization's Barracuda Message Archiver
- Barracuda Message Archiver HTTPS port number

In this article:

- Configuration
- Searching for Archived Messages
- Advanced Search Settings
- Message Results
- Replying to and Forwarding Archived Messages

Related Articles

- Install/Configure the Outlook Add-In

Secure Connectivity
The Barracuda Message Archiver Companion mobile application requires secure (HTTPS) connectivity to the Barracuda Message Archiver. If an insecure (HTTP) connection is attempted the mobile application is redirected to use *https:* with the configured secure port.

For existing mobile application users, if your URI was originally set up on an earlier firmware version, verify that the URI uses HTTPS. If the URI was set up using HTTP, use the steps in the section Configuration to update the URI. If the URI is *not* updated, users are automatically redirected to the secure, HTTPS protocol. This redirection may require an update to your network firewall rules to allow connectivity to complete on the secure port.

Certificates
When using HTTPS connectivity, if a self-signed or private certificate is in place on the Barracuda Message Archiver, your mobile phone operating system (OS) may require you to accept the private certificate before you can download content with the mobile OS download utility. The mechanism to add a private certificate to your mobile device varies; please consult your manufacturer instructions for more information.

The Barracuda Message Archiver mobile application allows you to perform various actions with your messages that are stored on your organization's Barracuda Message Archiver including:

- Search for archived messages based on email content, or constrain the search to a date range, a specific sender, or subject line content;
- Search deleted messages and emails no longer visible in your mail application;
- View and interact with (reply to, reply all, or forward) archived messages;
- Redeliver messages to your mailbox using the **Resend to Me** option.

These actions are available directly from your Android phone, allowing transparent access to, and interaction with, your archived messages.

Only archived messages are available for search with the Barracuda Message Archiver mobile application; non-email items such as calendar entries and contacts are not included in search results.

Configuration

To search your archived mail from your Android device, you must first enter your organization's Barracuda Message Archiver settings, as well as your email address and password.

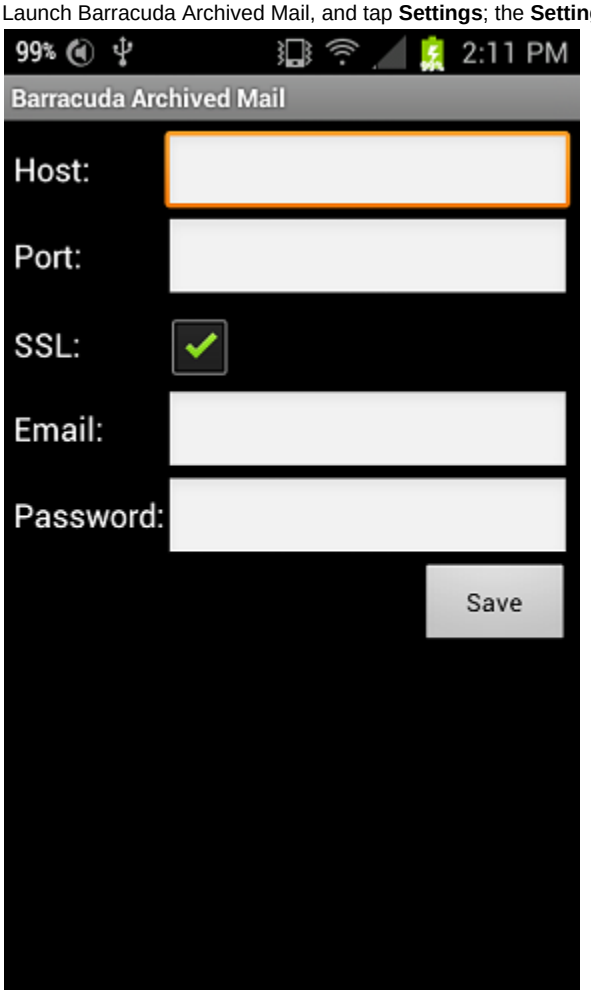
If you attempt to search archived messages before configuring the settings, an error displays. You must enter the following details to configure the

Android device:

- Barracuda Message Archiver hostname or IP address;
- Barracuda Message Archiver HTTPS port number;
- Specify whether the connection is secure;
- Your corporate email address from which messages are archived;
- Your email password.

Use the following steps to get started.

1. Before you can set up Archived Mail, you need your Barracuda Message Archiver URI from your system administrator. For example: `https://archiver.company.com:443`
2. Launch Barracuda Archived Mail, and tap **Settings**; the **Settings** page displays:



3. Tap in the **Host** field, and enter your organization's hostname or IP address. For example, enter: `archiver.company.com` or `192.168.200.200`
4. Tap in the **Port** field and enter the HTTPS port number. For example, enter `443`
5. In the **Email** field, tap and enter your email address from which to access archived messages. For example, enter: `myname@company.com`
6. Tap in the **Password** field, and enter your password for the specified email address.
7. Confirm your settings, and tap **Save**.
8. The **Settings saved** dialog displays; click **Ok**.

Searching for Archived Messages

Once configuration is complete, you can begin searching your archived emails.

> The Barracuda Message Archiver administrator can associate an LDAP user or group to a role and list of email addresses in the **USERS > LDAP User Add/Update** page. If addresses are excluded, and a configured user runs a search through the Barracuda Message Archiver Mobile Application, the following whitelist/blacklist rules apply:

- If an address is excluded (blacklisted), the address does not display unless the mail includes the user performing the search to assure that a user can always see their own mail.
- The exclusion rules always take precedence; addresses that are whitelisted are searchable only if the exclusion rules do not block the mail.
- If a user is not configured and is a member of a group, then the blacklist/whitelist rules assigned to that group apply to that user.
- If a user is assigned to a group, when the user logs in via the Outlook Add-In or Barracuda Message Archiver Mobile Application, only that user's mail displays. For example, if an LDAP user has the Auditor role, mail available to the Auditor role does not display.

Tap email at the top of the view, and tap in the Search field to display the keypad. Use the keypad to enter the desired keyword or search string; you must enter at least one keyword to perform a search:

Wildcards are not supported, and search is not case-sensitive.

Tap on the desired search criteria:

Criteria	Description
All	Returns all messages that contain the search string anywhere in the **From** field, subject line, or within the email content.
Subject	Returns messages that contain only the keyword in the subject line.
From	Returns messages that contain only the keyword in the **From** field.
Advanced	Restrict the results to a predefined date range; only those emails sent within the specified date(s) are returned in the search.

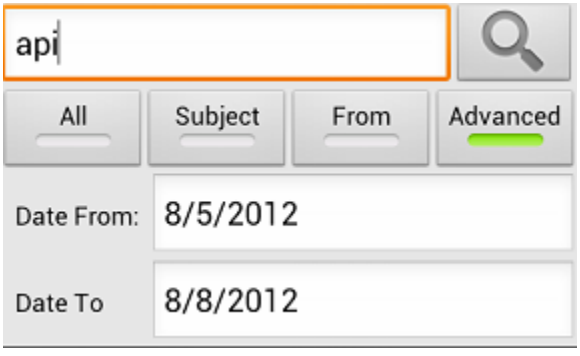
Once you specify the keyword and select the search criteria, tap the **Search** ( ) icon to display all messages matching your search criteria.

A search is performed on all of your mail folders including trash and deleted items.

Advanced Search Settings

To specify a specific date range in which to search, tap **Advanced** at the top of the view. The **Advanced Search** page displays the current date. The **Date From** and **Date To** fields populate with the current date.

1. Tap in the **Search** field, and enter your search criteria.
2. Tap in the **Date From** or **Date To** field, and enter the desired dates:



3. Tap the **Search** ( ) icon to display all messages matching your search criteria.

> The date selected in the **Date To** field must be the *same* or *later* date than the date selected in the **Date From** field.
>
> Any criteria specified in **Advanced** settings is used in conjunction with the criteria specified in the Search field; define your date range, and select **Advanced** from a Search to use the specified date range in conjunction with the keyword to search archived messages.

Message Results

All messages matching the specified criteria display in the search results directly below the search criteria.

Replying to and Forwarding Archived Messages

Once you have completed a search of your archived messages, you can view the message, reply to the message, or forward the message.

1. Tap on a message to display the full content in the window; the following options display across the bottom of the screen:
   - **Reply** - Sends an email response only to the message originator
   - **Reply All** - Sends an email response to the message originator and all recipients
   - **Forward** - Send a copy of the archived message to one or more new email addresses
2. Tap the desired option, enter the content of your message, and tap send.

Barracuda PST Collector

This article refers to the Barracuda Message Archiver release 3.1 or higher, except where noted.

Automated PST collection enables organizations to seamlessly meet litigation support and regulatory compliance requirements by simplifying the import of PSTs into the Barracuda Message Archiver. While the contents of individual PST files can be imported manually at any time, the Barracuda PST Collector automates the gathering and importing of pre-existing PST files from any directory on a Microsoft Windows-based system, minimizing the number of manual imports necessary to ensure that all emails are discoverable and included in the archive. The Barracuda PST Collector is available for Microsoft Windows-based systems only.

In this article:

- Components
- Configuration & Deployment Options
- Stages

Related Articles

- How to Assign and Unassign PST Files

Additional Resources

- Barracuda Networks Knowledgebase Solution # 0 0006097

> **PST Import Size Limit**
> For PST file imports initiated via the Barracuda Message Archiver web interface, there is a 100MB limit per mail item.

> **PST Assignment**
> In firmware 3.2 and earlier, PSTs are assigned to LDAP users. In firmware 3.5 and higher, the Administrator can assign a PST to a local user. Note that PST assignment allows visibility of the PST and access to folder names. Visibility of individual emails within the PST is still governed by the local user's email address and configured mail aliases, and email access is governed by these items being present in the mail headers.

Components

- **Barracuda PST Collector Server** - The server regulates PST transfers in your network to prevent potential network overload, and displays the location and status of all PST files (as reported by the Barracuda PST Collector clients). It runs as a Windows service on any Windows-based computer in your environment, and is controlled by an administrative console from which all PST collection is configured.
- **Barracuda PST Collector Client** - The client locates the PST files on the local system on which it is installed, and sends the PST files to the Barracuda Message Archiver. The client must be installed on all systems expected to contain PST files that require importing, and runs as a Windows service. However, it does not have any interface since all configurations are received from the Barracuda PST Collector Server.

  > All systems running the Barracuda PST Collector Client must have access to both the Barracuda PST Collector Server and the Barracuda Message Archiver. PST files are collected from the user's hard drives, not network shares or connected devices such as USB drives. If you want to collect PST files stored on network shares, the Client must be deployed upon the servers hosting your network shares, and on any external systems from which you want to add content. To import PST files from an external system (such as a remote user's laptop connected via VPN), or other machines with only intermittent network access, PST collection happens only when connectivity to the other systems is available. If connectivity is interrupted, the collection begins anew and does not resume in-place.

- **Barracuda Message Archiver** - The Barracuda Message Archiver server receives and process the imported PST files, and adds their contents to the archive.

To create the most comprehensive archive possible, Barracuda Networks recommends that you perform one-time PST collection using the Barracuda PST Collector to gather and import all historical emails saved in PST files into the Barracuda Message Archiver. Once PST collection is complete, the Barracuda PST Collector can be safely deactivated and uninstalled.

Configuration & Deployment Options

The following table describes the available configuration and deployment options:

Configuration Option	Associated Deployment
Option 1: Administrative template (ADM) with Group Policy (GPO) - *recommended*	Configure the Barracuda PST Collector Client using the ADM and deploy using GPO
Option 2: ADM with Custom Deployment	Configure the Barracuda PST Collector Client using the ADM and deploy using custom means, e.g., System Center Configuration Manager (SCCM)
Option 3: Command Line with Custom Deployment	Configure the Barracuda PST Collector Client using `-SERVER` at the command line, and deploy using custom means, e.g., SCCM

> **Important**
> All new installations require some initial synchronization tasks to be performed between the Microsoft Exchange Server and the Barracuda Message Archiver. These tasks, including the direct import of messages, stubbing, and folder synchronization, can take a fair amount of time to complete. The Barracuda Message Archiver prioritizes these tasks over processing collected PST files. Therefore, to reduce network traffic as well as potential load on the Barracuda Message Archiver, and to ensure that even the newest PST files are imported, it is *highly recommended* that PST collection begin *after* all such initial integration tasks are complete.

Stages

There are three main stages to PST collection:

- **Inventory** - The Barracuda PST Collector Client scans client systems for PST files, and creates an inventory of those files which is then submitted to the Barracuda PST Collector Server.
- **Transfer** - The Barracuda PST Collector Server authorizes and schedules each client to send their PST files to the Barracuda Message Archiver.
- **Import** - The Barracuda Message Archiver receives the PST files directly from the client systems and queues them for automatic import adding the contents of each PST file into the archive.

When the Barracuda PST Collector Client is initially installed, it registers against the designated Barracuda PST Collector Server. No PST files are reported or transmitted during this initial registration; thus, no discovered PST files display in the Admin Console. A list of registered clients is available from the **Reports > Registered Clients** menu. The Barracuda PST Collector Client then performs a one-time inventory of all PST files on the machine by scanning all non-network drives for files that have a PST extension and a valid signature. This inventory is then submitted to the Barracuda PST Collector Server, and the client system PST files are visible in the Admin Console.

> ⚠ **Caution**
> Any PST file created after this scan is *not* reported or transferred; it is essential to *disable* the creation of additional PST files prior to deploying the Barracuda PST Collector, particularly if PST collection is being done for compliance reasons.

At no time are the actual PST files transferred onto the Barracuda PST Collector Server; only the details of the files, such as the name, location, owner, size and dates/times of creation and last modification, are recorded.

Once the inventory is submitted, each client requests permission from the Barracuda PST Collector Server to initiate transfer of its PST files. The transfer policy configured in the Admin Console determines if, and when, the PST files are actually transferred:

- **Automatic** - All PSTs are approved for transfer.
- **Manual** - Only PST files marked in the Admin Console are approved for transfer; all other PST files remain listed in the display until they are either explicitly approved or a different transfer policy is selected.
- **Scheduled** - PST files are approved for transfer only during a specific time period.

If a file transfer is attempted on a PST file that is currently open, the client uses Microsoft's Volume Snapshot Service (VSS) to create a shadow copy of the volume containing the PST. The PST is then transferred from the shadow copy, and the shadow copy is deleted once PST collection is complete.

To prevent potential network congestion, the Barracuda PST Collector Server controls when approved PST file transfers occur. If an approved PST file transfer is not initiated at the time of the request, the Barracuda PST Collector Client resubmits the request in one hour. Once a transfer is approved, the client is sent the system information for the Barracuda Message Archiver. The client then coordinates directly with the Barracuda Message Archiver on the rate of file transfer to ensure maximum efficiency on both ends. If the system load on the Barracuda Message Archiver becomes too high, the client reinitiates contact in 10 minute intervals until all PST file transfers are complete.

Select your deployment:

- Option 1: ADM with GPO Deployment *(recommended)*
- Option 2: ADM with Custom Deployment
- Option 3: Command Line with Custom Deployment

Option 1 - ADM with GPO Deployment

This article refers to the Barracuda Message Archiver firmware 3.1 or higher, except where noted. Use this article to configure the Barracuda PST Collector Client using the Administrative template (ADM) and deploying through Group Policy (GPO). *This is the recommended method for deploying the PST Collector*. For additional deployment options, refer to the Barracuda PST Collector Deployment Options.

In this article:

- Enable PST Collection on the Barracuda Message Archiver
- Install the Barracuda PST Collector Server
- Deployment Options
- Set the 32-Bit MSI as Unavailable to 64-Bit Systems
- Install the Barracuda PST Collector Client
- Verify Barracuda PST Collector Client Installation
- Monitor and Verify PST Collection
- Assigned and Unassigned PSTs
- Manually Assigning a PST
- Verify Import of all Transferred PST Files
- Generate and Save a PST Collection Activity Report
- Uninstall the Barracuda PST Collector

Important
All new installations require some initial synchronization tasks to be performed between the Microsoft Exchange Server and the Barracuda Message Archiver. These tasks, including the direct import of messages, stubbing, and folder synchronization, can take a fair amount of time to complete. The Barracuda Message Archiver prioritizes these tasks over processing collected PST files. Therefore, to reduce network traffic as well as potential load on the Barracuda Message Archiver, and to ensure that even the newest PST files are imported, it is *highly recommended* that PST collection begin *after* all such initial integration tasks are complete.

Note that PST file imports initiated via the Barracuda Message Archiver web interface, there is a 100MB limit per mail item.

Enable PST Collection on the Barracuda Message Archiver

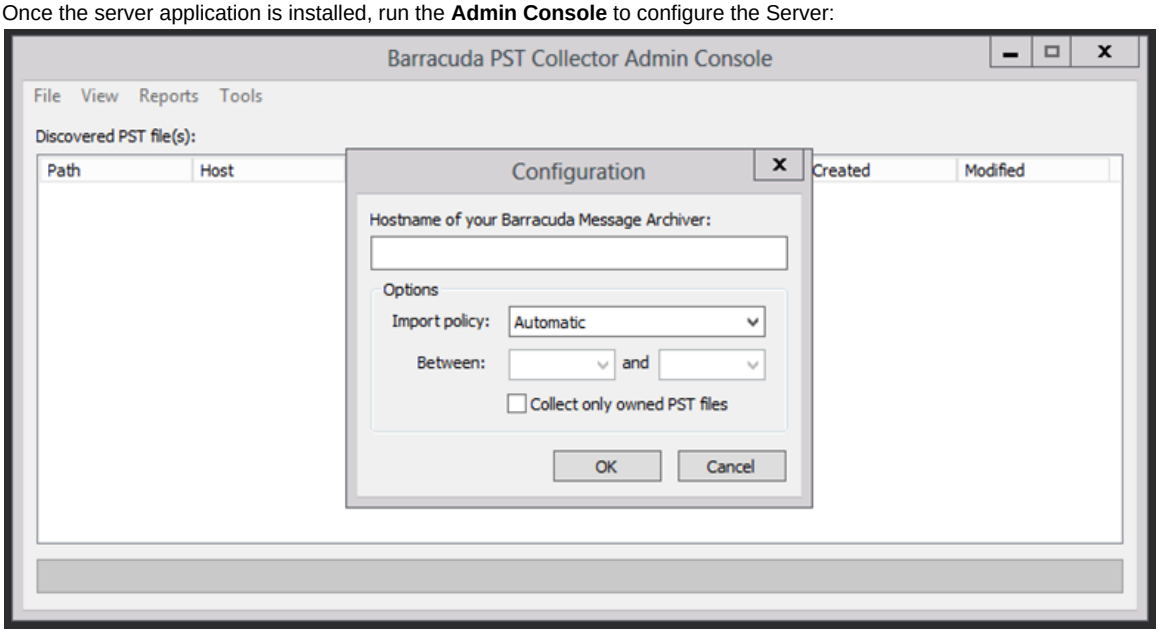
Use the following steps to enable PST collection on the Barracuda Message Archiver.

1. Log in to your Barracuda Message Archiver as admin, and navigate to the **MAIL SOURCES > PST Import** page.
2. In the **PST Import Options** section, set the **Enable PST Collector** option to *Yes*. Note that this feature *does not* require **Enable Local SMB Share** for PST imports to be enabled as the Collector uses a separate import directory.

Install the Barracuda PST Collector Server

Use the following steps to download, install, and configure the Barracuda PST Collector Server.

1. While still logged into your Barracuda Message Archiver as *admin*, navigate to the **USERS > Client Downloads** page.
2. Download and install the server application on a Microsoft Windows-based system in your environment that can be reached by all the systems on which the client application is to be deployed. Note that this need not be an actual server, nor does it need any special configuration; you can even use a virtual machine (VM) to function as the Server.
3. Once the server application is installed, run the **Admin Console** to configure the Server:



4. Enter the hostname (not the URI) of your Barracuda Message Archiver, for example, `archiver.company.com`, and select the desired import policy for PSTs:
   - **Automatic** - All PSTs are approved for transfer without any further interaction from a system administrator. Recommended.
   - **Manual** - A PST is approved for transfer only if that PST has been manually marked for transfer using the Admin Console. This setting always requires administrative input as each discovered PST file must be explicitly marked for import. This setting is typically used for importing only specific PST files, manually prioritizing specific PST files over others, or during testing of the Barracuda PST Collector in your environment.
   - **Scheduled** - A PST is approved for transfer only if the request occurs within a configured time window. This setting is typically used to restrict PST transfers to a specified time period when there is less traffic, such as after business hours.
5. To collect only PST files that are owned by domain users, set **Collect only owned PST files** to *On.*

Deployment Options

System Compatibility
If you install the 32-bit Barracuda PST Collector Client on a 64-bit operating system, and a PST file is in use on that 64-bit operating system, Microsoft Windows cannot use Volume Shadow Copy Service (VSS), therefore PST files cannot be collected until they are *no longer in use*. To resolve this issue, create two software deployment policies:

- One policy for the 32-bit client that targets only 32-bit machines, *and*
- One policy for the 64-bit client

A 64-bit .**msi** can target *only* 64-bit systems, whereas a 32-bit .**msi** can deploy to both 64- and 32-bit systems, or to just 32-bit systems.

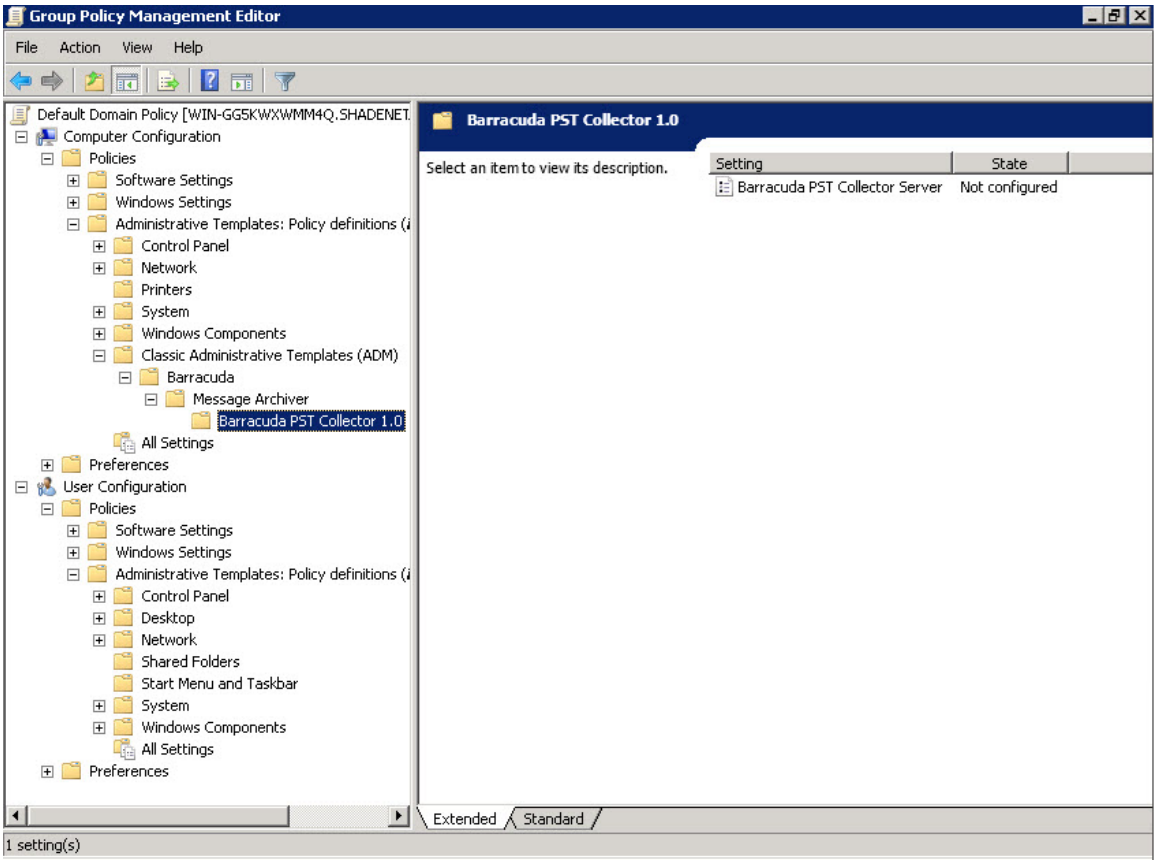
Before configuring your systems, determine the appropriate deployment based on the following table:

System	Deployment
32-bit Windows systems *only*	Deploy the 32-bit client MSI
64-bit Windows systems *only*	Deploy the 64-bit client MSI
Both 32- and 64-bit Windows systems	Deploy *both* the 32- and 64-bit client MSIs, but *configure* the 32-bit MSI to be unavailable to 64-bit systems using the steps outline in the section **Set the 32-Bit MSI as Unavailable to 64-Bit Systems**.

Configure the Barracuda PST Collector Client

Use the following steps to configure the Barracuda PST Collector Client.

1. While still logged into your Barracuda Message Archiver as *admin*, navigate to the **USERS > Client Downloads** page, and download the **PST Collector Deployment Kit**.
2. Extract the contents to an easily accessible location; the following files are included:
   - Barracuda PST Collector Client 32-bit version installer ending in _**x86.msi**
   - Barracuda PST Collector Client 64-bit version installer ending in _**x64.msi**
     Barracuda PST Collector administrator module **Barracuda PST Collector.adm**
3. Move (or copy) the **Barracuda PST Collector.adm** file to your local %systemroot%\inf directory, for example: C:\winnt\inf
4. While in the Group Policy Management Editor, navigate to **Computer Configuration > Administrative Templates,** and expand the **Barr acuda** node (for Windows 2008 Server, the policy appears under **Classic Administrative Templates (ADM)** as the templates are in ADM format).
5. Click **Message Archiver**, and click **Barracuda PST Collector**:



6. Double-click the **Barracuda PST Collector Server**.; the **Properties** window displays.
7. In the **Server Hostname** field, enter the hostname (not the URI) of the system where the Barracuda PST Collector Server is installed. For example, enter: `pstcolserver.domain.local`

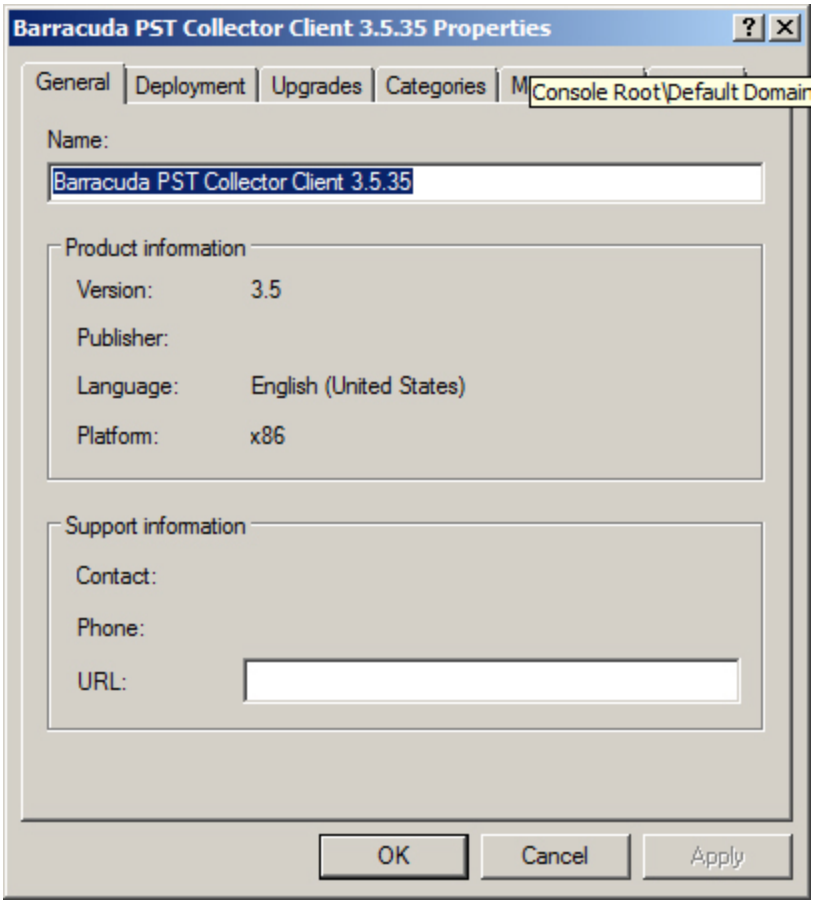
> The hostname must be resolvable and the system must be accessible by all machines on which the Barracuda PST Collector Client is to be deployed.

Set the 32-Bit MSI as Unavailable to 64-Bit Systems

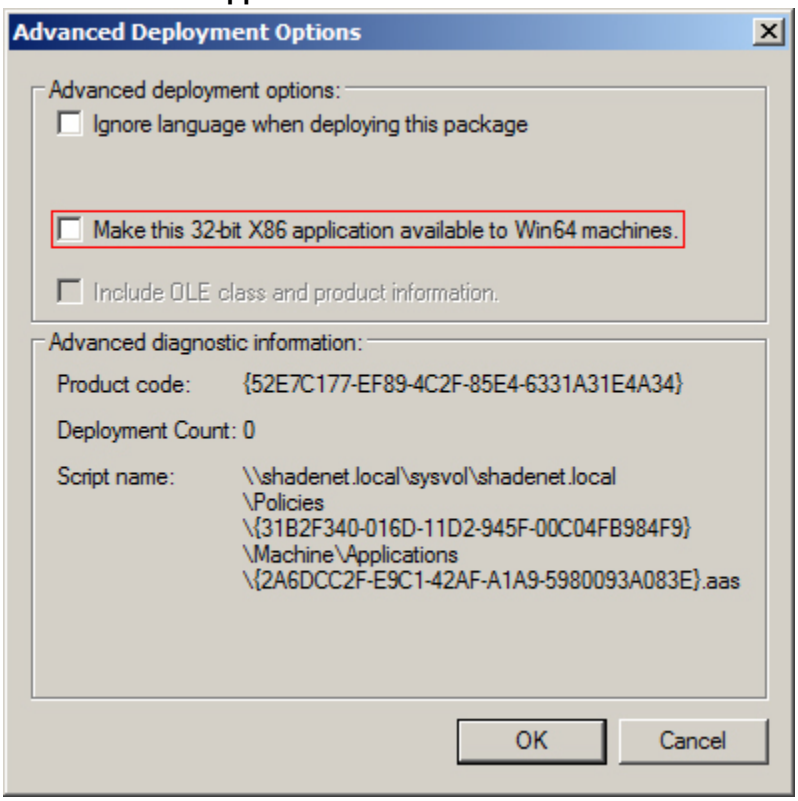
> **32- and 64-Bit Mixed Deployment Only**
> Use these steps *only* if you are deploying the Barracuda PST Collector to both 32- and 64-bit systems running in your environment.

If you are deploying to both 32- and 64-bit systems, install both the 32- and 64-bit client MSIs and configure the 32-bit MSI to be unavailable to 64-bit systems using the following steps:

1. While in the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Software Settings**, and click **Software Installation**.
2. Right-click **Barracuda PST Collector**, and click **Properties**:



3. Click the **Deployment** tab, and click **Advanced**. In the **Advanced deployment options** section, turn off **Make this 32-bit X86 application available to Win64 machines**:



4. Click **OK** to save your settings, and click **OK** to close the **Properties** window.

Install the Barracuda PST Collector Client

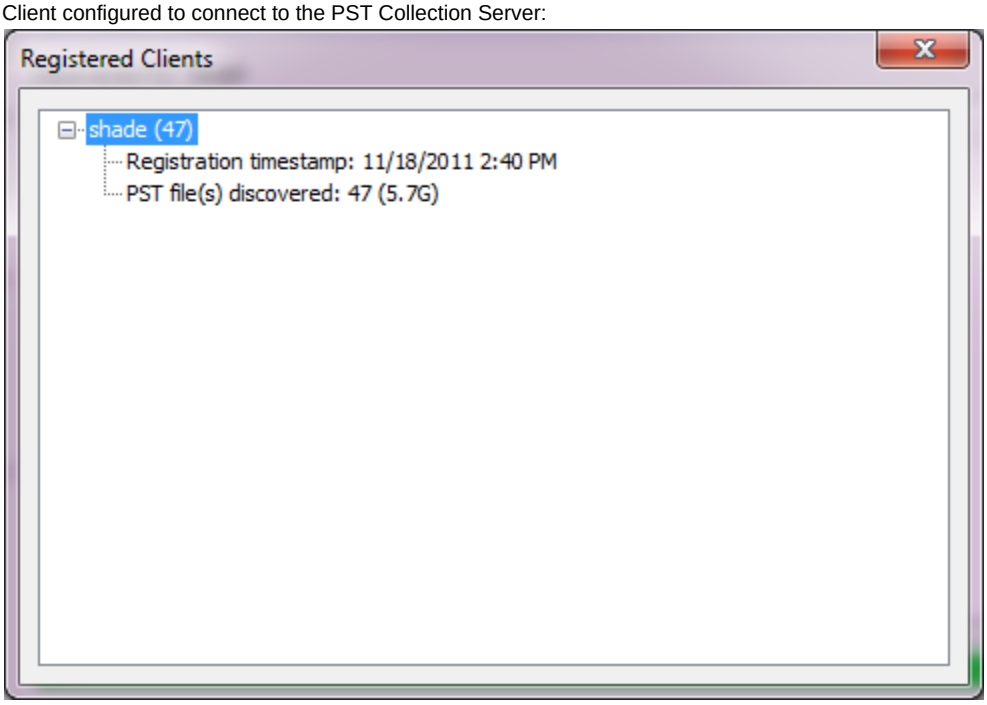
Use the following steps to download and install the Barracuda PST Collector Client.

1. Copy the **.msi** file(s) to a location or file share accessible to users.
2. Open the **Group Policy Management Editor** for the organizational unit (OU) that is to use the Barracuda PST Collector, e.g., the default domain policy.
3. Either *edit* the default policy or *create* a new policy object, and link it to the desired container. For example, the particular OU containing the computers on which the Barracuda PST Collector Client is to be installed.
4. In the **Group Policy Management Editor**, expand **Computer Configuration**.
5. Right-click on **Administrative Templates**, point to **All Tasks**, and click **Add/Remove Templates**.
6. Navigate to the %systemroot%\inf directory, select **Barracuda PST Collector.adm**, and click **Add**.
7. Start the **Group Policy Management Editor** for the domain in which you are installing the Barracuda PST Collector Client.
8. Either *edit* the default policy or *create* a new policy object, and link it to the desired container. For example, the particular OU containing the computers on which the Barracuda PST Collector Client is to be installed.
9. Navigate to **Computer Configuration > Software Settings > Software Installation**.
10. Right-click **Software Installation,** and click **New > Package**.
11. Enter the UNC path to the **.msi** file located in the shared folder. For example: `\\fileserver\deploy`
12. Click **OK**.

Verify Barracuda PST Collector Client Installation

Use the following steps to verify that the Barracuda PST Collector Client is installed and registered on all clients.

1. On the system where the Barracuda PST Collector Server is installed, go to **Start > Programs > Barracuda > Message Archiver > PST Collector** to open the PST Collector Admin Console.
2. From the **Reports** menu, click **Registered Clients**; a window displays a list of all systems currently running a Barracuda PST Collector Client configured to connect to the PST Collection Server:



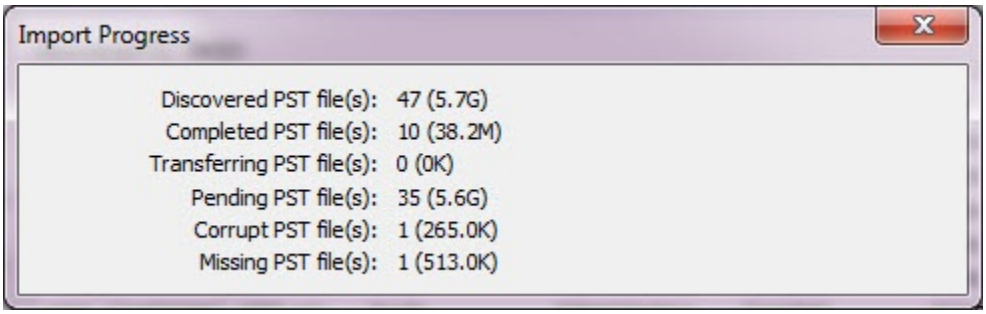
3. Restart the client system and verify the software installation policy has taken effect. The Barracuda PST Collector Client should be installed when you log in, with policies as configured on the Barracuda PST Collector Server already in place.
4. Group policies can take several minutes to post; if a system is not listed and you have used the **Group Policy Management Editor** to install the Barracuda PST Collector Client, run the following command to perform an immediate update: `gpupdate /force`
5. Once you run the command, restart the client system.
   Refresh the **Registered Clients** display on the Barracuda PST Collector Server, and verify the restarted system is registering correctly.

> Additional information on fixing GPO issues is available from the Microsoft website: http://technet.microsoft.com/en-us/library/cc775423.aspx

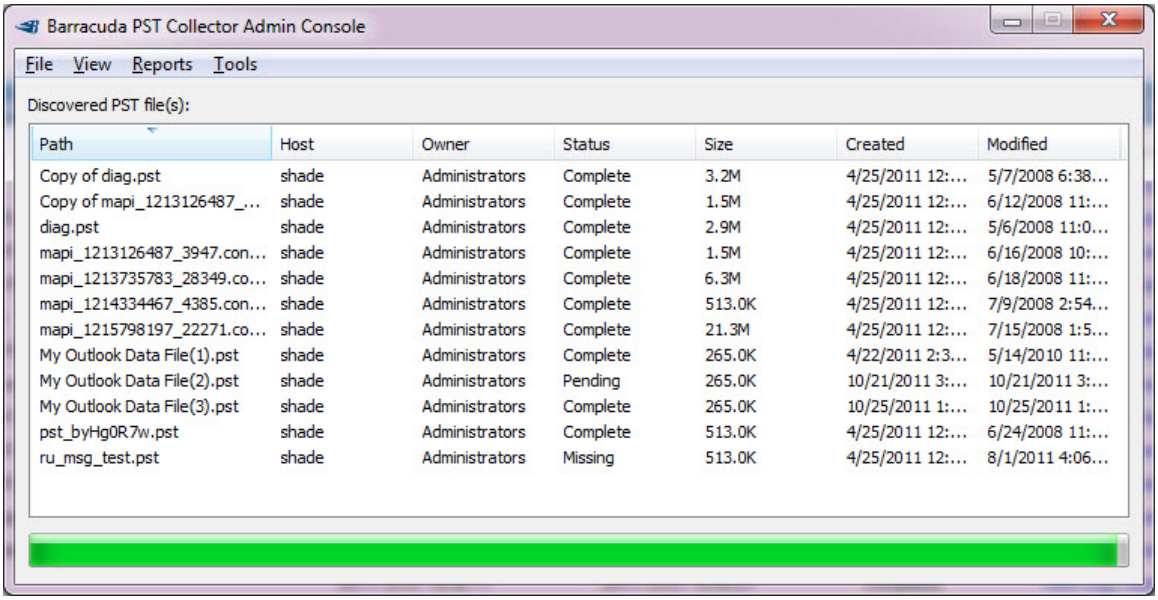
Monitor and Verify PST Collection

Use the following steps to monitor and verify PST collection.

1. On the system where the Barracuda PST Collector Server is installed, open the Admin Console (**Start > Programs > Barracuda > Message Archiver > PST Collector**).
2. From the **Reports** menu click **Import Progress**:


Import Progress
Discovered PST file(s): 47 (5.7G)
Completed PST file(s): 10 (38.2M)
Transferring PST file(s): 0 (0K)
Pending PST file(s): 35 (5.6G)
Corrupt PST file(s): 1 (265.0K)
Missing PST file(s): 1 (513.0K)

3. A window displays the number and size of the PST files that:
   - were discovered;
   - have completed transfer to the Barracuda Message Archiver;
   - are in the midst of a transfer;
   - are awaiting transfer;
   - are in some way corrupted.
4. Once imports are no longer in progress, verify that the number and size of the completed PST files are as expected in the **PST Collector Admin Console**:


Barracuda PST Collector Admin Console
File View Reports Tools
Discovered PST file(s):
Path Host Owner Status Size Created Modified
Copy of diag.pst shade Administrators Complete 3.2M 4/25/2011 12:... 5/7/2008 6:38...
Copy of mapi_1213126487_... shade Administrators Complete 1.5M 4/25/2011 12:... 6/12/2008 11:...
diag.pst shade Administrators Complete 2.9M 4/25/2011 12:... 5/6/2008 11:0...
mapi_1213126487_3947.con... shade Administrators Complete 1.5M 4/25/2011 12:... 6/16/2008 10:...
mapi_1213735783_28349.co... shade Administrators Complete 6.3M 4/25/2011 12:... 6/18/2008 11:...
mapi_1214334467_4385.con... shade Administrators Complete 513.0K 4/25/2011 12:... 7/9/2008 2:54...
mapi_1215798197_22271.co... shade Administrators Complete 21.3M 4/25/2011 12:... 7/15/2008 1:5...
My Outlook Data File(1).pst shade Administrators Complete 265.0K 4/22/2011 2:3... 5/14/2010 11:...
My Outlook Data File(2).pst shade Administrators Pending 265.0K 10/21/2011 3:... 10/21/2011 3:...
My Outlook Data File(3).pst shade Administrators Complete 265.0K 10/25/2011 1:... 10/25/2011 1:...
pst_byHg0R7w.pst shade Administrators Complete 513.0K 4/25/2011 12:... 6/24/2008 11:...
ru_msg_test.pst shade Administrators Missing 513.0K 4/25/2011 12:... 8/1/2011 4:06...

5. If there are PST files that failed to complete due to corruption or other errors, return to the main Admin Console window. From the **View** menu select **Filter**, and click **Show Corrupt**. A list of all such PST files displays in the main window along with detailed information including the owner, the originating client system, and creation and last modification dates. Independent investigation may be necessary to perform for each PST file that failed to import as there can be a variety of reasons for the failure including (but not limited to):
   - the client system does not have, or does not allow, adequate access to the PST file location;
   - the PST file is too large for transfer;
   - the PST file is still in use.

> Error messages are found in various logs on the client system including those in the installation directory. If you are unable to find a cause for the PST import errors, consider enabling verbose logging or contact Barracuda Networks Technical Support for further assistance.

Assigned and Unassigned PSTs

When the Barracuda PST Collector submits a PST file to the Barracuda Message Archiver, the user's security identifier (SID), obtained from the

Windows User Profile, is collected and stored.

> If no user SID is available at the time the PST is sent to the PST Server, automatic user assignment *is not* performed. However, if auto-assignment cannot be made, the administrator can manually assign a PST to an active AD user by right-clicking on the PST file in the **BASIC > Search** page in the **PSTs and Tags** tab.
>
> In firmware 3.5 and higher, the Administrator can assign a PST to a local user. Note that PST assignment allows visibility of the PST and access to folder names. Visibility of individual emails within the PST is still governed by the local user's email address and configured mail aliases, and email access is governed by these items being present in the mail headers.

Once a PST file is enabled for processing, if the SID is resolvable via the configured LDAP source, the PST file is assigned to the appropriate user based on the LDAP lookup, and displays in the **Assigned PSTs** folder in the **BASIC > Search** page in the **PSTs and Tags** tab. If the SID cannot be resolved through LDAP lookup, the PST file is processed but is not assigned to a user. The PST file displays in the **Unassigned PSTs** folder in the **BASIC > Search** page in the **PSTs and Tags** tab.

> Emails processed from an 'unassigned' PST file are available in the **Search** page and are available to both the Message Archiver administrator and to any user whose email address or aliases are included in the email headers.

Manually Assigning a PST

To manually assign an unassigned PST file to a user already displayed in the **Assigned PSTs** folder, use the following steps:

1. Log in to the Barracuda Message Archiver as the administrator, and go to the **BASIC > Search** page.
2. Click the **PSTs and Tags** tab, and open the **Unassigned PSTs** folder.
3. Click on the unassigned PST and drag it to a user name listed in the **Assigned PSTs** folder.

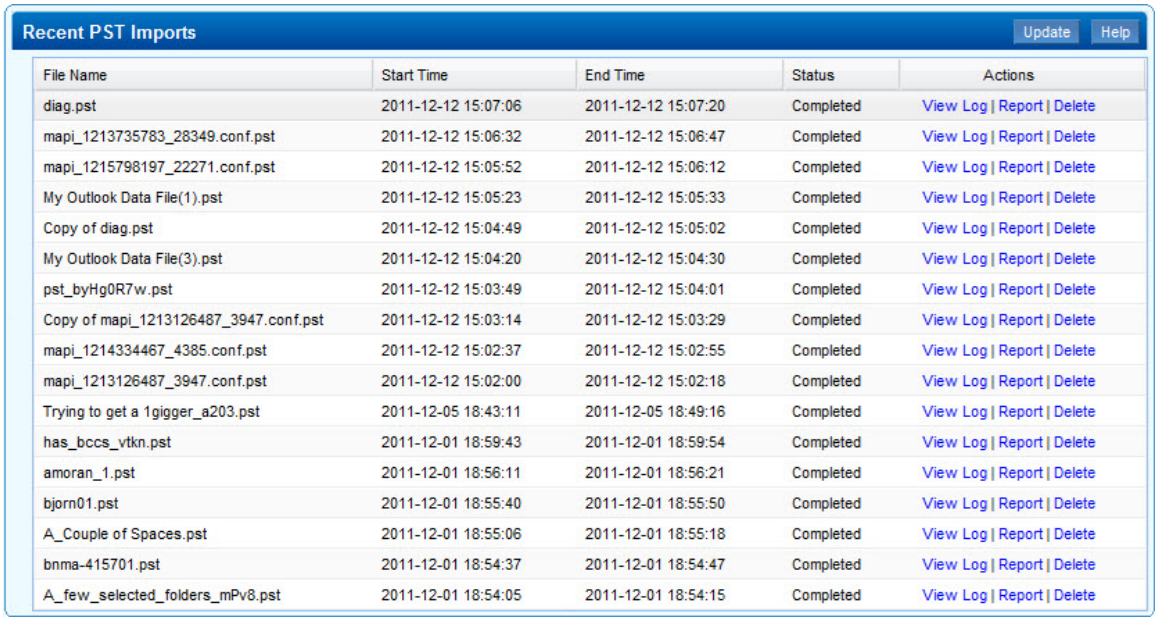
To manually assign the PST file to a user not displayed in the **Assigned PSTs** folder, use the following steps:

1. Log in to the Barracuda Message Archiver as the administrator, and go to the **BASIC > Search** page.
2. Click the **PSTs and Tags** tab, navigate to and right-click the PST file to assign, and then click **Assign PST**.
3. In the **Assign PST** dialog box, enter at least three characters of the email address to which to assign the PST.
4. The **Search for User** field populates with all matching users; click on the user to which to assign the PST file, and click **OK**.

Verify Import of all Transferred PST Files

Use the following steps to confirm that all PST files are correctly transferred to the Barracuda Message Archiver, and verify that the contents of each PST file has been extracted and imported into the archive.

1. Log into the Barracuda Message Archiver, and navigate to the **MAIL SOURCES > PST Import** page.
2. In the **Recent PST Imports** section, verify the status for all listed PST files displays as **Completed** *:*



File Name	Start Time	End Time	Status	Actions
diag.pst	2011-12-12 15:07:06	2011-12-12 15:07:20	Completed	View Log | Report | Delete
mapi_1213735783_28349.conf.pst	2011-12-12 15:06:32	2011-12-12 15:06:47	Completed	View Log | Report | Delete
mapi_1215798197_22271.conf.pst	2011-12-12 15:05:52	2011-12-12 15:06:12	Completed	View Log | Report | Delete
My Outlook Data File(1).pst	2011-12-12 15:05:23	2011-12-12 15:05:33	Completed	View Log | Report | Delete
Copy of diag.pst	2011-12-12 15:04:49	2011-12-12 15:05:02	Completed	View Log | Report | Delete
My Outlook Data File(3).pst	2011-12-12 15:04:20	2011-12-12 15:04:30	Completed	View Log | Report | Delete
pst_byHg0R7w.pst	2011-12-12 15:03:49	2011-12-12 15:04:01	Completed	View Log | Report | Delete
Copy of mapi_1213126487_3947.conf.pst	2011-12-12 15:03:14	2011-12-12 15:03:29	Completed	View Log | Report | Delete
mapi_1214334467_4385.conf.pst	2011-12-12 15:02:37	2011-12-12 15:02:55	Completed	View Log | Report | Delete
mapi_1213126487_3947.conf.pst	2011-12-12 15:02:00	2011-12-12 15:02:18	Completed	View Log | Report | Delete
Trying to get a 1gigger_a203.pst	2011-12-05 18:43:11	2011-12-05 18:49:16	Completed	View Log | Report | Delete
has_bccs_vtkn.pst	2011-12-01 18:59:43	2011-12-01 18:59:54	Completed	View Log | Report | Delete
amoran_1.pst	2011-12-01 18:56:11	2011-12-01 18:56:21	Completed	View Log | Report | Delete
bjorn01.pst	2011-12-01 18:55:40	2011-12-01 18:55:50	Completed	View Log | Report | Delete
A_Couple of Spaces.pst	2011-12-01 18:55:06	2011-12-01 18:55:18	Completed	View Log | Report | Delete
bnma-415701.pst	2011-12-01 18:54:37	2011-12-01 18:54:47	Completed	View Log | Report | Delete
A_few_selected_folders_mPv8.pst	2011-12-01 18:54:05	2011-12-01 18:54:15	Completed	View Log | Report | Delete

3. For any listed file, including files that did not complete, click the **View Log** link to display a log of what transpired during the import, or click the **Report** link to view a summary of the imported data.

Generate and Save a PST Collection Activity Report

1. On the system where the Barracuda PST Collector Server is installed, and go to **Start > Programs > Barracuda > Message Archiver > PST Collector** to open the PST Collector Admin Console.
2. From the **File** menu, click **Export Discovered PST Data**.
3. Select the name and location where you want to store the data displayed in the main window. The file is saved in **CSV** format, suitable for reading by Microsoft Excel or similar program.

Uninstall the Barracuda PST Collector

Use the following steps to uninstall the Barracuda PST Collector from the client systems and server:

1. Using the **Group Policy Management Editor**, uninstall the Barracuda PST Collector Client from all systems to which it was deployed.
2. Uninstall the Barracuda PST Collector Server from the system where it was installed, typically via the **Add or Remove Programs** utility.

Option 2 - ADM with Custom Deployment

This article refers to the Barracuda Message Archiver release 3.1 or higher, and describes how to configure the Barracuda PST Collector Client using the Administrative template (ADM) and deploying through custom means, e.g., System Center Configuration Manager (SCCM).

For additional deployment options, refer to the Barracuda PST Collector Deployment Options.

In this article:

- Enable PST Collection on the Barracuda Message Archiver
- Install the Barracuda PST Collector Server
- Configure the Barracuda PST Collector Client
- Create the PST Collector Software Distribution Package
- Verify Barracuda PST Collector Client Installation
- Monitor and Verify PST Collection
- Assigned and Unassigned PSTs
- Manually Assigning a PST
- Verify Import of all Transferred PST Files
- Generate and Save a PST Collection Activity Report
- Uninstall the Barracuda PST Collector

Important
All new installations require some initial synchronization tasks to be performed between the Microsoft Exchange Server and the Barracuda Message Archiver. These tasks, including the direct import of messages, stubbing, and folder synchronization, can take a fair amount of time to complete. The Barracuda Message Archiver prioritizes these tasks over processing collected PST files. Therefore, to reduce network traffic as well as potential load on the Barracuda Message Archiver, and to ensure that even the newest PST files are imported, it is *highly recommended* that PST collection begin *after* all such initial integration tasks are complete.

Note that PST file imports initiated via the Barracuda Message Archiver web interface, there is a 100MB limit per mail item.

Enable PST Collection on the Barracuda Message Archiver

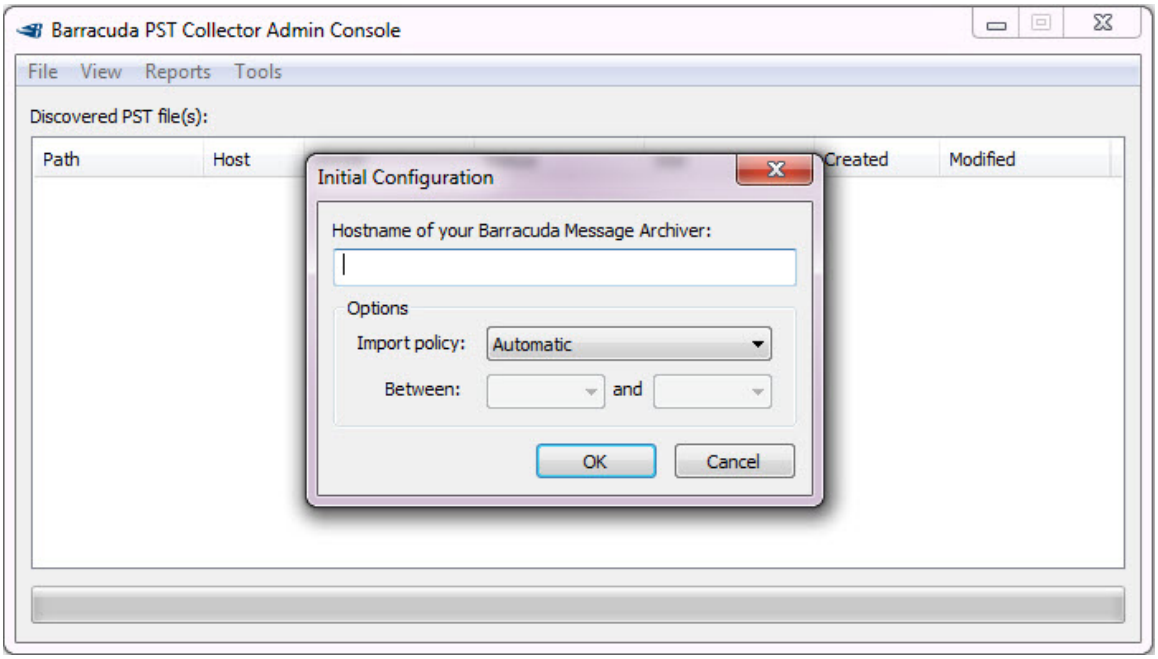
Use the following steps to enable PST collection on the Barracuda Message Archiver.

1. Log into your Barracuda Message Archiver as *admin*, and navigate to the **MAIL SOURCES > PST Import** page.
2. In the **PST Import Options** section, set the **Enable PST Collector** option to *Yes*. Note that this feature *does not* require **Enable Local SMB Share** for PST imports to be enabled as the Collector uses a separate import directory.

Install the Barracuda PST Collector Server

Use the following steps to download, install, and configure the Barracuda PST Collector Server.

1. While still logged into your Barracuda Message Archiver as *admin*, navigate to the **USERS > Client Downloads** page.
2. Download and install the server application on a Microsoft Windows-based system in your environment that can be reached by all the systems on which the client application is to be deployed. Note that this need not be an actual server, nor does it need any special configuration; you can even use a virtual machine (VM) to function as the Server.
3. Once the server application is installed, run the **Admin Console** to configure the Server:



4. Enter the hostname (not the URI) of your Barracuda Message Archiver, for example, `archiver.company.com`, and select the desired import policy for PSTs:
    - ***Automatic*** - All PSTs are approved for transfer without any further interaction from a system administrator. Recommended.
    - ***Manual*** - A PST is approved for transfer only if that PST has been manually marked for transfer using the Admin Console. This setting always requires administrative input as each discovered PST file must be explicitly marked for import. This setting is typically used for importing only specific PST files, manually prioritizing specific PST files over others, or during testing of the Barracuda PST Collector in your environment.
    - ***Scheduled*** - A PST is approved for transfer only if the request occurs within a configured time window. This setting is typically used to restrict PST transfers to a specified time period when there is less traffic, such as after business hours.

Configure the Barracuda PST Collector Client

Use the following steps to configure the Barracuda PST Collector Client.

1. While still logged into your Barracuda Message Archiver as *admin*, navigate to the **USERS > Client Downloads** page, and download the **PST Collector Deployment Kit**.
2. Extract the contents to an easily accessible location; the following files are included:
    - Barracuda PST Collector Client 32bit version installer ending in **_x86.msi**
    - Barracuda PST Collector Client 64bit version installer ending in **_x64.msi**
    - Barracuda PST Collector administrator module **Barracuda PST Collector.adm**
3. Move (or copy) the **Barracuda PST Collector.adm** file to your local %systemroot%\inf directory, for example: C:\winnt\inf
4. Copy the **.msi** file(s) to a location or file share accessible to users.

Create the PST Collector Software Distribution Package

Use the following steps to configure the Barracuda PST Collector Client. Open the **Configuration Manager Console** and navigate to **System Center Configuration Manager > Site Database > Computer Management > Software Distribution**, and complete the following:

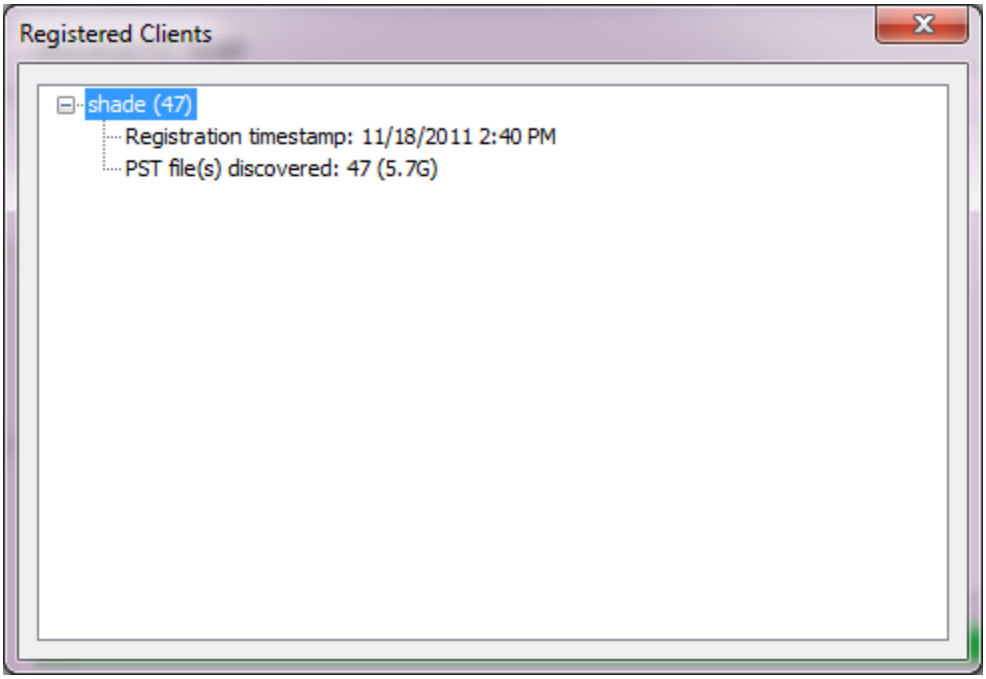
1. Go to **System Center Configuration Manager > Site Database > Computer Management > Collections** and create a Collection to enable the selection of the computer resources of the targeted user computers.
2. Go to **System Center Configuration Manager > Site Database > Computer Management > Packages** and use the **New Package** Wiz ard to create a distribution package specifying the UNC path of the **.msi** file(s) to be deployed.
3. Use the **New Distribution Points Wizard** to select the distribution server(s).

4. Use the **New Advertisements Wizard** to create a job to distribute the package to users; use the **Schedule** tab to select dates and times to run the package.

Verify Barracuda PST Collector Client Installation

Use the following steps to verify that the Barracuda PST Collector Client is installed and registered on all clients.

1. On the system where the Barracuda PST Collector Server is installed, open the Admin Console (**Start > Programs > Barracuda > Message Archiver > PST Collector**).
2. From the **Reports** menu, click **Registered Clients**; a window displays a list of all systems currently running a Barracuda PST Collector Client configured to connect to the PST Collection Server:

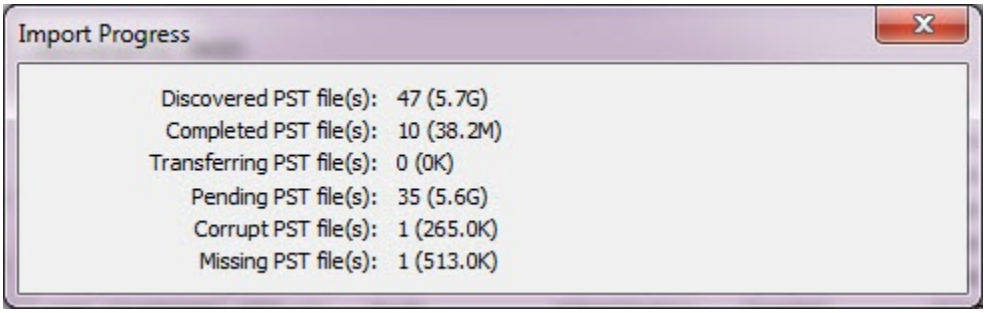


3. Once the software is installed, it displays in the list of registered clients.
4. Refresh the **Registered Clients** display on the Barracuda PST Collector Server, and verify the restarted system is registering correctly.

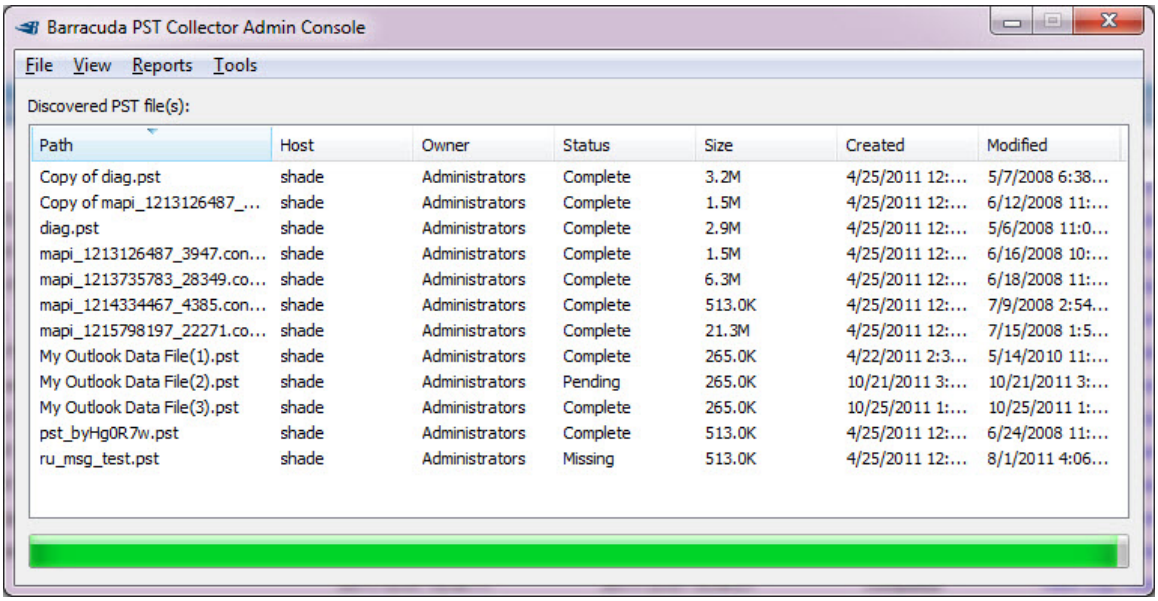
Monitor and Verify PST Collection

Use the following steps to monitor and verify PST collection.

1. On the system where the Barracuda PST Collector Server is installed, open the Admin Console (**Start > Programs > Barracuda > Message Archiver > PST Collector**).
2. From the **Reports** menu click **Import Progress**:


Import Progress
Discovered PST file(s): 47 (5.7G)
Completed PST file(s): 10 (38.2M)
Transferring PST file(s): 0 (0K)
Pending PST file(s): 35 (5.6G)
Corrupt PST file(s): 1 (265.0K)
Missing PST file(s): 1 (513.0K)

   A window displays the number and size of the PST files that:
   - were discovered;
   - have completed transfer to the Barracuda Message Archiver;
   - are in the midst of a transfer;
   - are awaiting transfer;
3. Once imports are no longer in progress, verify that the number and size of the completed PST files are as expected in the **PST Collector Admin Console**:


Barracuda PST Collector Admin Console
File View Reports Tools
Discovered PST file(s):
Path Host Owner Status Size Created Modified
Copy of diag.pst shade Administrators Complete 3.2M 4/25/2011 12:... 5/7/2008 6:38...
Copy of mapi_1213126487_... shade Administrators Complete 1.5M 4/25/2011 12:... 6/12/2008 11:...
diag.pst shade Administrators Complete 2.9M 4/25/2011 12:... 5/6/2008 11:0...
mapi_1213126487_3947.con... shade Administrators Complete 1.5M 4/25/2011 12:... 6/16/2008 10:...
mapi_1213735783_28349.co... shade Administrators Complete 6.3M 4/25/2011 12:... 6/18/2008 11:...
mapi_1214334467_4385.con... shade Administrators Complete 513.0K 4/25/2011 12:... 7/9/2008 2:54...
mapi_1215798197_22271.co... shade Administrators Complete 21.3M 4/25/2011 12:... 7/15/2008 1:5...
My Outlook Data File(1).pst shade Administrators Complete 265.0K 4/22/2011 2:3... 5/14/2010 11:...
My Outlook Data File(2).pst shade Administrators Pending 265.0K 10/21/2011 3:... 10/21/2011 3:...
My Outlook Data File(3).pst shade Administrators Complete 265.0K 10/25/2011 1:... 10/25/2011 1:...
pst_byHg0R7w.pst shade Administrators Complete 513.0K 4/25/2011 12:... 6/24/2008 11:...
ru_msg_test.pst shade Administrators Missing 513.0K 4/25/2011 12:... 8/1/2011 4:06...

4. If there are PST files that failed to complete due to corruption or other errors, return to the main Admin Console window. From the **View** menu select **Filter**, and click **Show Corrupt**. A list of all such PST files displays in the main window along with detailed information including the owner, the originating client system, and creation and last modification dates. Independent investigation may be necessary to perform for each PST file that failed to import as there can be a variety of reasons for the failure including (but not limited to):
    - the client system does not have, or does not allow, adequate access to the PST file location;
    - the PST file is too large for transfer;
    - the PST file is still in use.

    > Error messages are found in various logs on the client system including those in the installation directory. If you are unable to find a cause for the PST import errors, consider enabling verbose logging or contact Barracuda Networks Technical Support for further assistance.

Assigned and Unassigned PSTs

When the Barracuda PST Collector submits a PST file to the Barracuda Message Archiver, the user's security identifier (SID), obtained from the Windows User Profile, is collected and stored.

> If no user SID is available at the time the PST is sent to the PST Server, automatic user assignment *is not* performed. However, if auto-assignment cannot be made, the administrator can manually assign a PST to an active AD user by right-clicking on the PST file in the **BASIC > Search** page in the **PSTs and Tags** tab.

Once a PST file is enabled for processing, if the SID is resolvable via the configured LDAP source, the PST file is assigned to the appropriate user based on the LDAP lookup, and displays in the **Assigned PSTs** folder in the **BASIC > Search** page in the **PSTs and Tags** tab. If the SID cannot be resolved through LDAP lookup, the PST file is processed but is not assigned to a user. The PST file displays in the **Unassigned PSTs** folder in the **BASIC > Search** page in the **PSTs and Tags** tab.

> Emails processed from an 'unassigned' PST file are available in the **Search** page and are available to both the Message Archiver administrator and to any user whose email address or aliases are included in the email headers.

Manually Assigning a PST

To manually assign an unassigned PST file to a user already displayed in the **Assigned PSTs** folder, use the following steps:

1. Log in to the Barracuda Message Archiver as the administrator, and go to the **BASIC > Search** page.
2. Click the **PSTs and Tags** tab, and open the **Unassigned PSTs** folder.
3. Click on the unassigned PST and drag it to a user name listed in the **Assigned PSTs** folder.

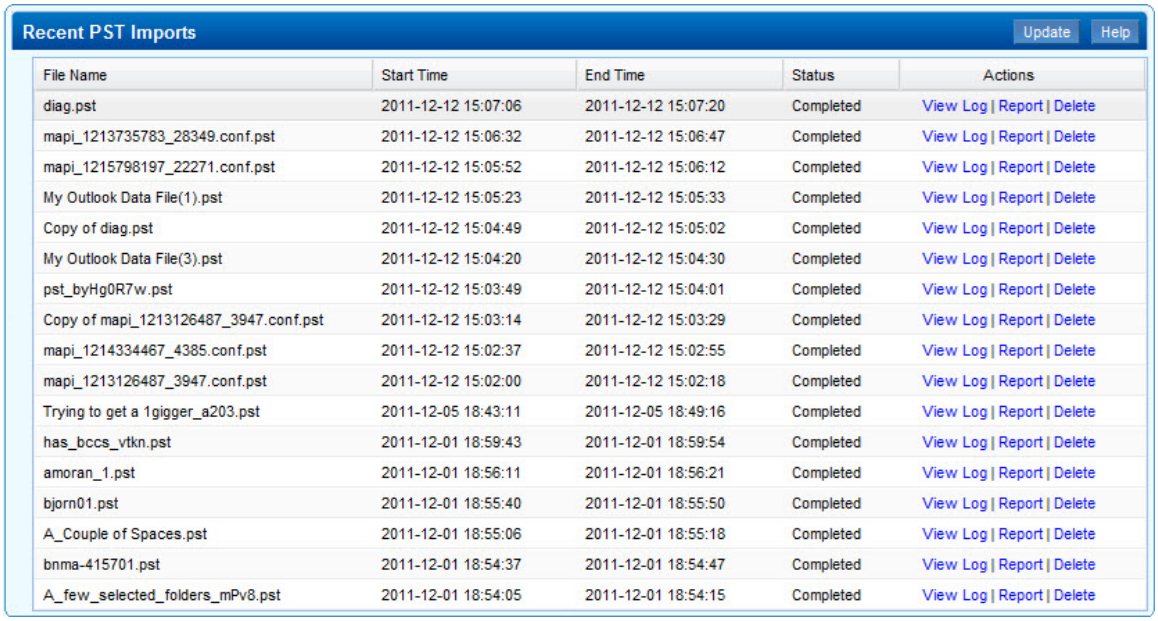
To manually assign the PST file to a user not displayed in the **Assigned PSTs** folder, use the following steps:

1. Log in to the Barracuda Message Archiver as the administrator, and go to the **BASIC > Search** page.
2. Click the **PSTs and Tags** tab, navigate to and right-click the PST file to assign, and then click **Assign PST**.
3. In the **Assign PST** dialog box, enter at least three characters of the email address to which to assign the PST.
4. The **Search for User** field populates with all matching users; click on the user to which to assign the PST file, and click **OK**.

Verify Import of all Transferred PST Files

Use the following steps to confirm that all PST files are correctly transferred to the Barracuda Message Archiver, and verify that the contents of each PST file has been extracted and imported into the archive.

1. Log into your Barracuda Message Archiver as *admin*, and navigate to the **MAIL SOURCES > PST Import** page.
2. In the **Recent PST Imports** section, verify the status for all listed PST files displays as *Completed:*



File Name	Start Time	End Time	Status	Actions
diag.pst	2011-12-12 15:07:06	2011-12-12 15:07:20	Completed	View Log | Report | Delete
mapi_1213735783_28349.conf.pst	2011-12-12 15:06:32	2011-12-12 15:06:47	Completed	View Log | Report | Delete
mapi_1215798197_22271.conf.pst	2011-12-12 15:05:52	2011-12-12 15:06:12	Completed	View Log | Report | Delete
My Outlook Data File(1).pst	2011-12-12 15:05:23	2011-12-12 15:05:33	Completed	View Log | Report | Delete
Copy of diag.pst	2011-12-12 15:04:49	2011-12-12 15:05:02	Completed	View Log | Report | Delete
My Outlook Data File(3).pst	2011-12-12 15:04:20	2011-12-12 15:04:30	Completed	View Log | Report | Delete
pst_byHg0R7w.pst	2011-12-12 15:03:49	2011-12-12 15:04:01	Completed	View Log | Report | Delete
Copy of mapi_1213126487_3947.conf.pst	2011-12-12 15:03:14	2011-12-12 15:03:29	Completed	View Log | Report | Delete
mapi_1214334467_4385.conf.pst	2011-12-12 15:02:37	2011-12-12 15:02:55	Completed	View Log | Report | Delete
mapi_1213126487_3947.conf.pst	2011-12-12 15:02:00	2011-12-12 15:02:18	Completed	View Log | Report | Delete
Trying to get a 1gigger_a203.pst	2011-12-05 18:43:11	2011-12-05 18:49:16	Completed	View Log | Report | Delete
has_bccs_vtkn.pst	2011-12-01 18:59:43	2011-12-01 18:59:54	Completed	View Log | Report | Delete
amoran_1.pst	2011-12-01 18:56:11	2011-12-01 18:56:21	Completed	View Log | Report | Delete
bjorn01.pst	2011-12-01 18:55:40	2011-12-01 18:55:50	Completed	View Log | Report | Delete
A_Couple of Spaces.pst	2011-12-01 18:55:06	2011-12-01 18:55:18	Completed	View Log | Report | Delete
bnma-415701.pst	2011-12-01 18:54:37	2011-12-01 18:54:47	Completed	View Log | Report | Delete
A_few_selected_folders_mPv8.pst	2011-12-01 18:54:05	2011-12-01 18:54:15	Completed	View Log | Report | Delete

3. For any listed file, including files that did not complete, click the **ViewLog** link to display a log of what transpired during the import, or click the *Report* link to view a summary of the imported data.

Generate and Save a PST Collection Activity Report

1. On the system where the Barracuda PST Collector Server is installed, open the Admin Console (**Start > Programs > Barracuda > Message Archiver > PST Collector**).
2. From the **File** menu, click **Export Discovered PST Data**.
3. Select the name and location where you want to store the data displayed in the main window. The file is saved in **CSV** format, suitable for reading by Microsoft Excel or similar program.

Uninstall the Barracuda PST Collector

Use the following steps to uninstall the Barracuda PST Collector from the client systems and server:

1. Open the **Configuration Manager Console** and navigate to **System Center Configuration Manager > Site Database > Computer Management > Software Distribution**.
2. Go to **Advertisements** and delete the Advertisement you created to deploy the **.msi** file(s).

Option 3 - Command Line with Custom Deployment

This article refers to the Barracuda Message Archiver release 3.1 or higher. Use this deployment option if you do not want to deploy with ADM and GPO. This article describes how to deploy the PST Collector using custom means such as the System Center Configuration Manager (SCCM).

For additional deployment options, refer to the Barracuda PST Collector Deployment Options.

In this article:

- Enable PST Collection on the Barracuda Message Archiver

- Install the Barracuda PST Collector Server
- Configure the Barracuda PST Collector Client
- Create the PST Collector Software Distribution Package
- Verify Barracuda PST Collector Client Installation
- Monitor and Verify PST Collection
- Assigned and Unassigned PSTs
- Manually Assigning a PST
- Verify Import of all Transferred PST Files
- Generate and Save a PST Collection Activity Report
- Uninstall the Barracuda PST Collector

Important
All new installations require some initial synchronization tasks to be performed between the Microsoft Exchange Server and the Barracuda Message Archiver. These tasks, including the direct import of messages, stubbing, and folder synchronization, can take a fair amount of time to complete. The Barracuda Message Archiver prioritizes these tasks over processing collected PST files. Therefore, to reduce network traffic as well as potential load on the Barracuda Message Archiver, and to ensure that even the newest PST files are imported, it is *highly recommended* that PST collection begin *after* all such initial integration tasks are complete.

Note that PST file imports initiated via the Barracuda Message Archiver web interface, there is a 100MB limit per mail item.

Enable PST Collection on the Barracuda Message Archiver

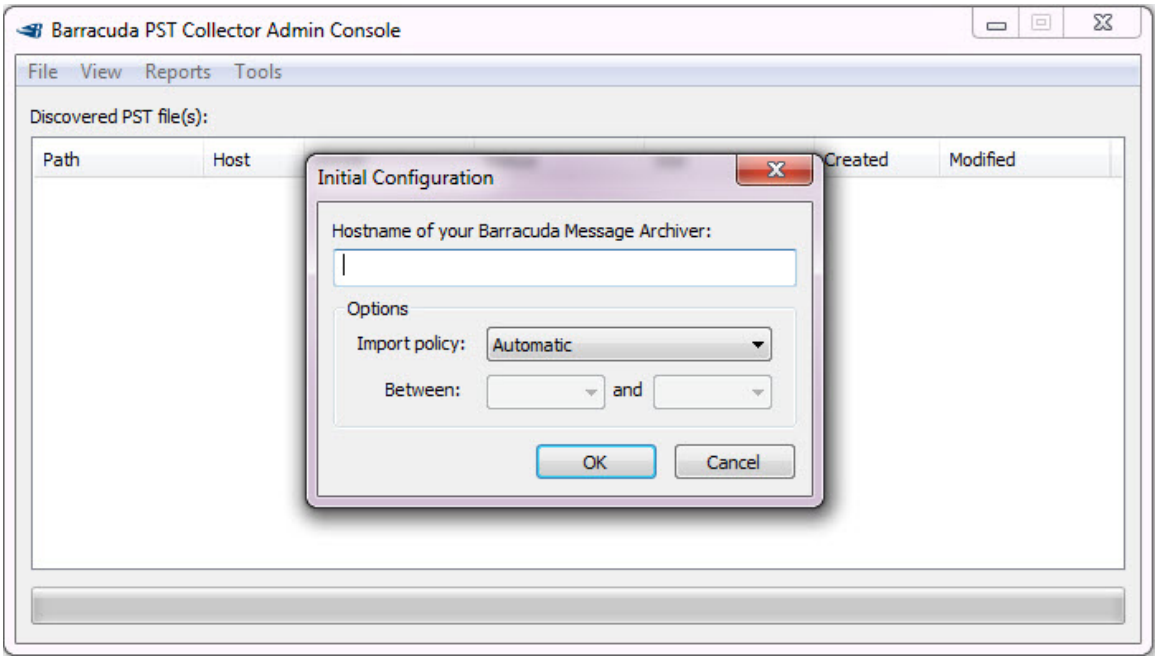
Use the following steps to enable PST collection on the Barracuda Message Archiver.

1. Log into your Barracuda Message Archiver as *admin*, and navigate to the **MAIL SOURCES > PST Import** page.
2. In the **PST Import Options** section, set the **Enable PST Collector** option to *Yes*. Note that this feature *does not* require **Enable Local SMB Share** for PST imports to be enabled as the Collector uses a separate import directory.

Install the Barracuda PST Collector Server

Use the following steps to download, install, and configure the Barracuda PST Collector Server.

1. While still logged into your Barracuda Message Archiver as *admin*, navigate to the **USERS > Client Downloads** page.
2. Download and install the server application on a Microsoft Windows-based system in your environment that can be reached by all the systems on which the client application is to be deployed. Note that this need not be an actual server, nor does it need any special configuration; you can even use a virtual machine (VM) to function as the Server.
3. Once the server application is installed, run the **Admin Console** to configure the Server:



4. Enter the hostname (not the URI) of your Barracuda Message Archiver, for example, `http://archiver.company.com`, and select the

desired import policy for PSTs:

- ***Automatic*** - All PSTs are approved for transfer without any further interaction from a system administrator. Recommended.
- ***Manual -*** A PST is approved for transfer only if that PST has been manually marked for transfer using the Admin Console. This setting always requires administrative input as each discovered PST file must be explicitly marked for import. This setting is typically used for importing only specific PST files, manually prioritizing specific PST files over others, or during testing of the Barracuda PST Collector in your environment.
- ***Scheduled*** - A PST is approved for transfer only if the request occurs within a configured time window. This setting is typically used to restrict PST transfers to a specified time period when there is less traffic, such as after business hours.

Configure the Barracuda PST Collector Client

Use the following steps to configure the Barracuda PST Collector Client.

1. While still logged into your Barracuda Message Archiver as *admin*, navigate to the **USERS > Client Downloads** page, and download the **PST Collector Deployment Kit**.
2. Extract the contents to an easily accessible location; the following files are included:
   - Barracuda PST Collector Client 32-bit version installer ending in _**x86.msi**
   - Barracuda PST Collector Client 64-bit version installer ending in _**x64.msi**
   - Barracuda PST Collector administrator module **Barracuda PST Collector.adm**
3. Move (or copy) the **Barracuda PST Collector.adm** file to your local %systemroot%\inf directory, for example: C:\winnt\inf
4. Copy the **.msi** file(s) to a location or file share accessible to users

Create the PST Collector Software Distribution Package

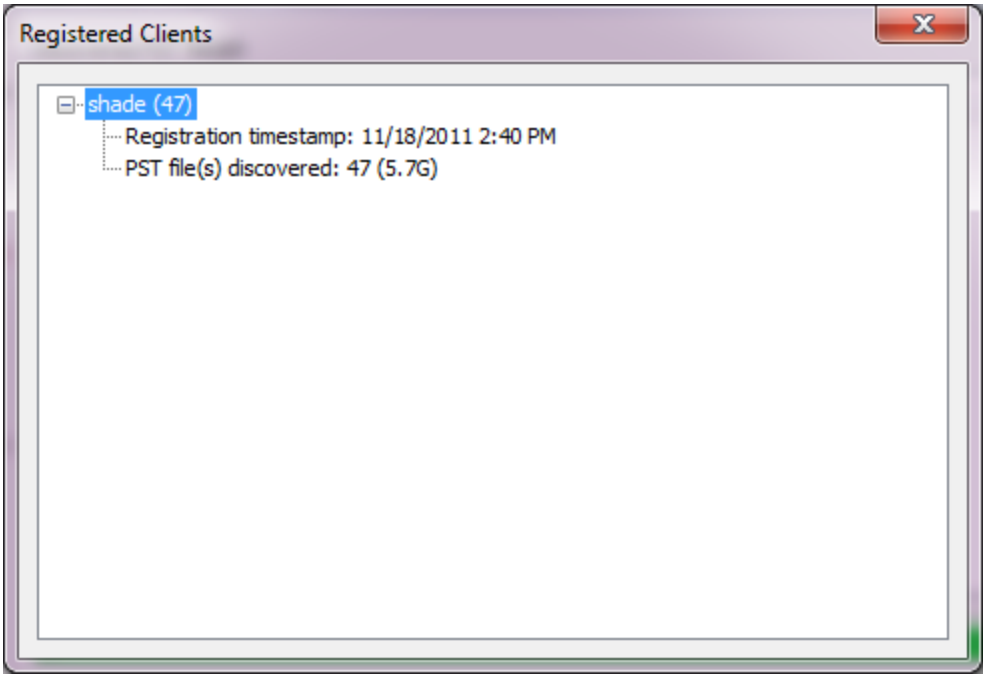
Use the following steps to configure the Barracuda PST Collector Client.

1. Open the **Configuration Manager Console** and navigate to **System Center Configuration Manager > Site Database > Computer Management > Packages:**
   - Specify the general information, data source, distribution settings, and any other desired information for the new package.
   - In the **Data Source** page, specify the UNC path of the **.msi** file(s) to be deployed.
2. Go to **System Center Configuration Manager > Site Database > Computer Management > Software Distribution > Package** and open the package created in the previous step.
3. Right-click **Programs**, point to **New**, and click **Program**.
4. In the **New Program Wizard**, enter the following in the **Command line** field:
   - For 64-bit distribution:
     `msiexec /i BarPstColClient-<version>_x64.msi SERVER= <server FQDN>`
     for example:
     `msiexec /i BarPstColClient-3.1.0_x64.msi SERVER=localhost`
   - For 32-bit distribution
     `msiexec /i BarPstColClient-<version>_x86.msi SERVER= <server FQDN>`
     for example:
     `msiexec /i BarPstColClient-3.1.0_x86.msi SERVER=localhost`
5. Enter the remaining details as necessary.
6. For the Package, open the **Properties** dialog box, and click the **Requirements** tab to specify client platforms on which the program is to run.
7. Use the **New Distribution Points Wizard** to select the distribution server(s).
8. Use the **New Advertisements Wizard** to create a job to distribute the package to users; use the **Schedule** tab to select dates and times when you want to run the package.

Verify Barracuda PST Collector Client Installation

Use the following steps to verify that the Barracuda PST Collector Client is installed and registered on all clients.

1. On the system where the Barracuda PST Collector Server is installed, open the Admin Console (**Start > Programs > Barracuda > Message Archiver > PST Collector**).
2. From the **Reports** menu, click **Registered Clients**; a window displays a list of all systems currently running a Barracuda PST Collector Client configured to connect to the PST Collection Server:

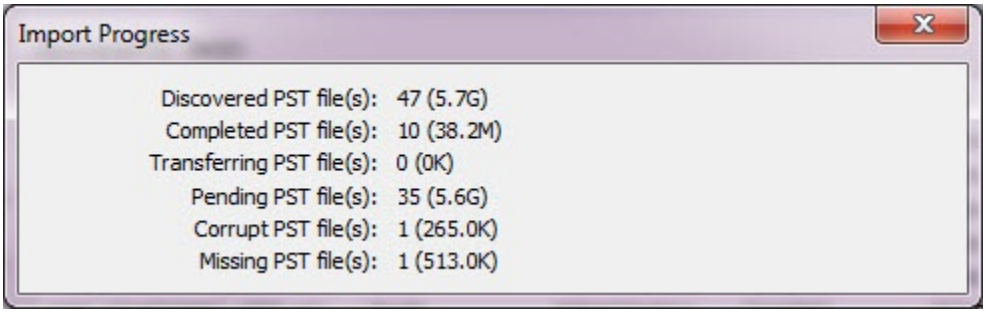


3. Once the software is installed, it displays in the list of registered clients.
4. Refresh the **Registered Clients** display on the Barracuda PST Collector Server, and verify the restarted system is registering correctly.

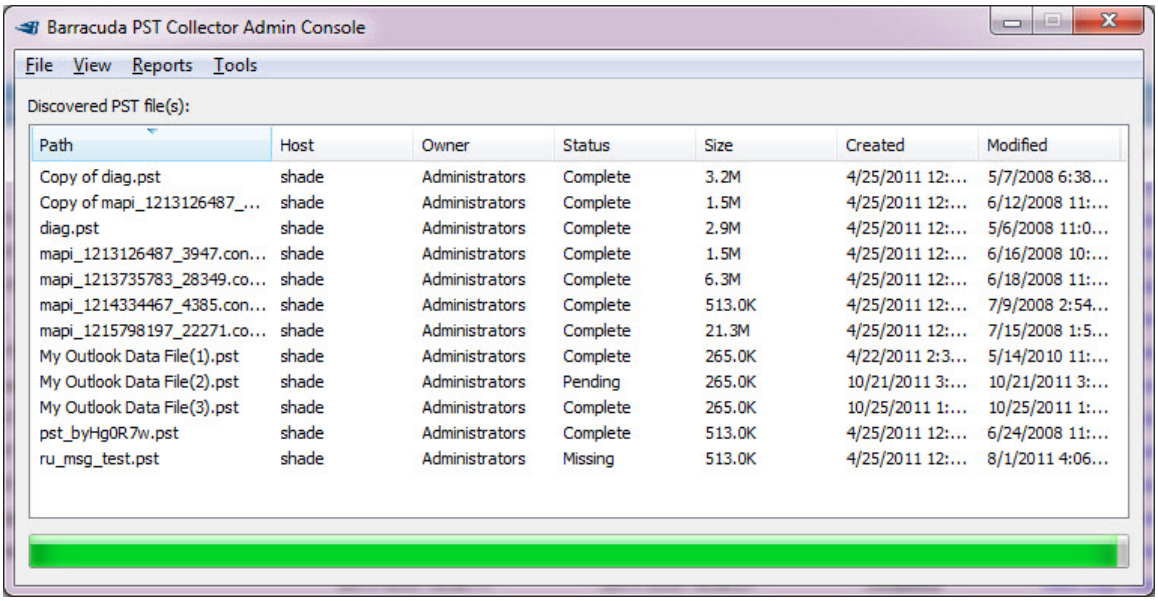
Monitor and Verify PST Collection

Use the following steps to monitor and verify PST collection.

1. On the system where the Barracuda PST Collector Server is installed, open the Admin Console (**Start > Programs > Barracuda > Message Archiver > PST Collector**).
2. From the **Reports** menu click **Import Progress**:


Import Progress
Discovered PST file(s): 47 (5.7G)
Completed PST file(s): 10 (38.2M)
Transferring PST file(s): 0 (0K)
Pending PST file(s): 35 (5.6G)
Corrupt PST file(s): 1 (265.0K)
Missing PST file(s): 1 (513.0K)

   A window displays the number and size of the PST files that:
   - were discovered;
   - have completed transfer to the Barracuda Message Archiver;
   - are in the midst of a transfer;
   - are awaiting transfer;
3. Once imports are no longer in progress, verify that the number and size of the completed PST files are as expected in the **PST Collector Admin Console:**


Barracuda PST Collector Admin Console
File View Reports Tools
Discovered PST file(s):
Path Host Owner Status Size Created Modified
Copy of diag.pst shade Administrators Complete 3.2M 4/25/2011 12:... 5/7/2008 6:38...
Copy of mapi_1213126487_... shade Administrators Complete 1.5M 4/25/2011 12:... 6/12/2008 11:...
diag.pst shade Administrators Complete 2.9M 4/25/2011 12:... 5/6/2008 11:0...
mapi_1213126487_3947.con... shade Administrators Complete 1.5M 4/25/2011 12:... 6/16/2008 10:...
mapi_1213735783_28349.co... shade Administrators Complete 6.3M 4/25/2011 12:... 6/18/2008 11:...
mapi_1214334467_4385.con... shade Administrators Complete 513.0K 4/25/2011 12:... 7/9/2008 2:54...
mapi_1215798197_22271.co... shade Administrators Complete 21.3M 4/25/2011 12:... 7/15/2008 1:5...
My Outlook Data File(1).pst shade Administrators Complete 265.0K 4/22/2011 2:3... 5/14/2010 11:...
My Outlook Data File(2).pst shade Administrators Pending 265.0K 10/21/2011 3:... 10/21/2011 3:...
My Outlook Data File(3).pst shade Administrators Complete 265.0K 10/25/2011 1:... 10/25/2011 1:...
pst_byHg0R7w.pst shade Administrators Complete 513.0K 4/25/2011 12:... 6/24/2008 11:...
ru_msg_test.pst shade Administrators Missing 513.0K 4/25/2011 12:... 8/1/2011 4:06...

4. If there are PST files that failed to complete due to corruption or other errors, return to the main Admin Console window. From the **View** menu select **Filter**, and click **Show Corrupt**. A list of all such PST files displays in the main window along with detailed information including the owner, the originating client system, and creation and last modification dates. Independent investigation may be necessary to perform for each PST file that failed to import as there can be a variety of reasons for the failure including (but not limited to):
    - the client system does not have, or does not allow, adequate access to the PST file location;
    - the PST file is too large for transfer;
    - the PST file is still in use

    > Error messages are found in various logs on the client system including those in the installation directory. If you are unable to find a cause for the PST import errors, consider enabling verbose logging or contact Barracuda Networks Technical Support for further assistance.

Assigned and Unassigned PSTs

When the Barracuda PST Collector submits a PST file to the Barracuda Message Archiver, the user's security identifier (SID), obtained from the Windows User Profile, is collected and stored.

> If no user SID is available at the time the PST is sent to the PST Server, automatic user assignment *is not* performed. However, if auto-assignment cannot be made, the administrator can manually assign a PST to an active AD user by right-clicking on the PST file in the **BASIC > Search** page in the **PSTs and Tags** tab.

Once a PST file is enabled for processing, if the SID is resolvable via the configured LDAP source, the PST file is assigned to the appropriate user based on the LDAP lookup, and displays in the **Assigned PSTs** folder in the **BASIC > Search** page in the **PSTs and Tags** tab. If the SID cannot be resolved through LDAP lookup, the PST file is processed but is not assigned to a user. The PST file displays in the **Unassigned PSTs** folder in the **BASIC > Search** page in the **PSTs and Tags** tab.

> Emails processed from an 'unassigned' PST file are available in the **Search** page and are available to both the Message Archiver administrator and to any user whose email address or aliases are included in the email headers.

Manually Assigning a PST

To manually assign an unassigned PST file to a user already displayed in the **Assigned PSTs** folder, use the following steps:

1. Log in to the Barracuda Message Archiver as the administrator, and go to the **BASIC > Search** page.
2. Click the **PSTs and Tags** tab, and open the **Unassigned PSTs** folder.
3. Click on the unassigned PST and drag it to a user name listed in the **Assigned PSTs** folder.

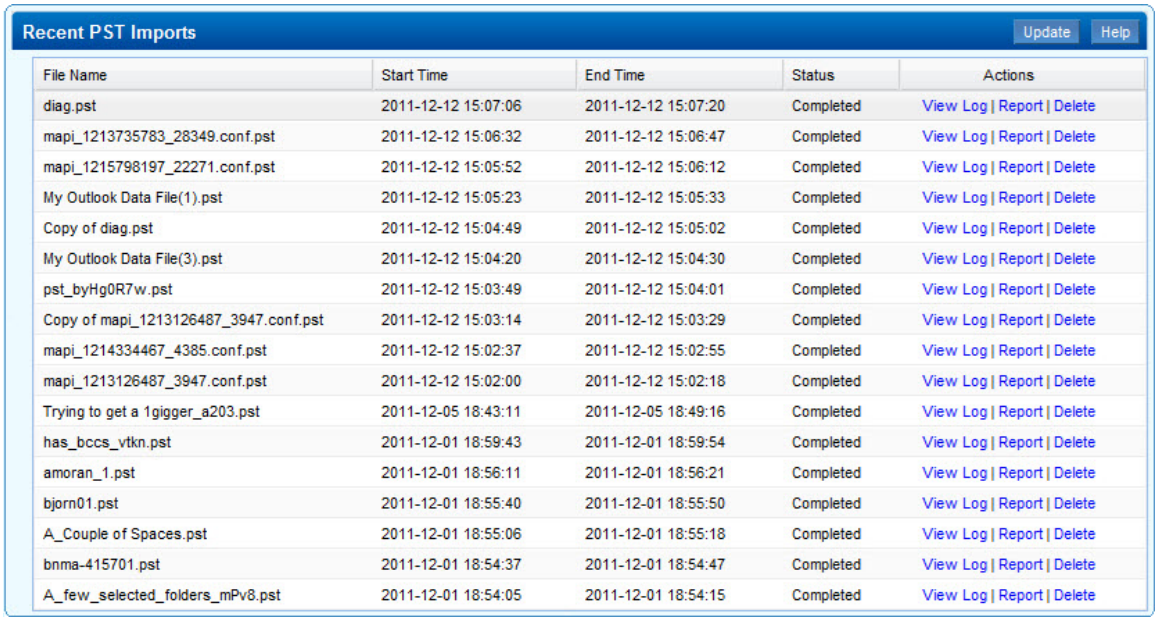
To manually assign the PST file to a user not displayed in the **Assigned PSTs** folder, use the following steps:

1. Log in to the Barracuda Message Archiver as the administrator, and go to the **BASIC > Search** page.
2. Click the **PSTs and Tags** tab, navigate to and right-click the PST file you want to assign, and then click **Assign PST**.
3. In the **Assign PST** dialog box, enter at least three characters of the email address to which to assign the PST.
4. The **Search for User** field populates with all matching users; click on the user to which to assign the PST file, and click **OK**.

Verify Import of all Transferred PST Files

Use the following steps to confirm that all PST files are correctly transferred to the Barracuda Message Archiver, and verify that the contents of each PST file has been extracted and imported into the archive.

1. Log into your Barracuda Message Archiver as *admin*, and navigate to the **MAIL SOURCES > PST Import** page.
2. In the **Recent PST Imports** section, verify the status for all listed PST files displays as **Completed**:



Recent PST Imports — Update | Help

File Name	Start Time	End Time	Status	Actions
diag.pst	2011-12-12 15:07:06	2011-12-12 15:07:20	Completed	View Log | Report | Delete
mapi_1213735783_28349.conf.pst	2011-12-12 15:06:32	2011-12-12 15:06:47	Completed	View Log | Report | Delete
mapi_1215798197_22271.conf.pst	2011-12-12 15:05:52	2011-12-12 15:06:12	Completed	View Log | Report | Delete
My Outlook Data File(1).pst	2011-12-12 15:05:23	2011-12-12 15:05:33	Completed	View Log | Report | Delete
Copy of diag.pst	2011-12-12 15:04:49	2011-12-12 15:05:02	Completed	View Log | Report | Delete
My Outlook Data File(3).pst	2011-12-12 15:04:20	2011-12-12 15:04:30	Completed	View Log | Report | Delete
pst_byHg0R7w.pst	2011-12-12 15:03:49	2011-12-12 15:04:01	Completed	View Log | Report | Delete
Copy of mapi_1213126487_3947.conf.pst	2011-12-12 15:03:14	2011-12-12 15:03:29	Completed	View Log | Report | Delete
mapi_1214334467_4385.conf.pst	2011-12-12 15:02:37	2011-12-12 15:02:55	Completed	View Log | Report | Delete
mapi_1213126487_3947.conf.pst	2011-12-12 15:02:00	2011-12-12 15:02:18	Completed	View Log | Report | Delete
Trying to get a 1gigger_a203.pst	2011-12-05 18:43:11	2011-12-05 18:49:16	Completed	View Log | Report | Delete
has_bccs_vtkn.pst	2011-12-01 18:59:43	2011-12-01 18:59:54	Completed	View Log | Report | Delete
amoran_1.pst	2011-12-01 18:56:11	2011-12-01 18:56:21	Completed	View Log | Report | Delete
bjorn01.pst	2011-12-01 18:55:40	2011-12-01 18:55:50	Completed	View Log | Report | Delete
A_Couple of Spaces.pst	2011-12-01 18:55:06	2011-12-01 18:55:18	Completed	View Log | Report | Delete
bnma-415701.pst	2011-12-01 18:54:37	2011-12-01 18:54:47	Completed	View Log | Report | Delete
A_few_selected_folders_mPv8.pst	2011-12-01 18:54:05	2011-12-01 18:54:15	Completed	View Log | Report | Delete

3. For any listed file, including files that did not complete, click the **View Log** link to display a log of what transpired during the import, or click the **Report** link to view a summary of the imported data.

Generate and Save a PST Collection Activity Report

1. On the system where the Barracuda PST Collector Server is installed, open the Admin Console (**Start > Programs > Barracuda > Message Archiver > PST Collector**).
2. From the **File** menu, click **Export Discovered PST Data**.
3. Select the name and location where you want to store the data displayed in the main window. The file is saved in **CSV** format, suitable for reading by Microsoft Excel or similar program.

Uninstall the Barracuda PST Collector

Use the following steps to uninstall the Barracuda PST Collector from the client systems and server:

1. Open the **Configuration Manager Console** and navigate to **System Center Configuration Manager > Site Database > Computer Management > Software Distribution**.
2. Go to **Advertisements** and delete the Advertisement you created to deploy the **.msi** file(s).

Barracuda Message Archiver Stand-Alone Search Utility

In this Section

- Barracuda Message Archiver Stand Alone Search Utility - Windows Deployment
- Barracuda Message Archiver Stand-Alone Search Utility for Windows
- Barracuda Message Archiver Stand-Alone Search Utility for Mac OS X

Barracuda Message Archiver Stand Alone Search Utility - Windows Deployment

This article refers to the Barracuda Message Archiver release 3.1 or higher.

Installation

Use the following steps to install the Barracuda Message Archiver Standalone Search Addin Deployment Kit.

1. Log in to the Barracuda Message Archiver as an administrator.
2. Navigate to the **USERS > Client Downloads** page, and download the **StandAlone Search Utility Deployment Kit**.
3. Extract the contents to an easily accessible location; the deployment kit contains the following:
   - Barracuda Message Archiver StandAlone Search Utility installer (**BmaSaSearch-version.msi**)
   - Barracuda Message Archiver StandAlone Search Utility Administrator module (**Barracuda Message Archiver Search version.adm**)
   - A copy of this document in PDF format
4. Move (or copy) the **Barracuda Message Archiver Search version.adm** file to your local %systemroot%\inf, directory, typically found in: **c:\winnt\inf**
5. Copy the .**msi** file to a location that is accessible by your users.
6. Open the Group Policy Object (GPO) Editor for the organization that is to use the Barracuda Message Archiver StandAlone Search Utility (e.g., the default domain policy).
7. Either edit the default policy or create a new policy object, and link it to the desired container. For example, the particular organizational unit (OU) containing the computers on which the utility is to be installed.
8. Expand **Computer Configuration**, rightclick **Administrative Templates**, select **All Tasks**, and click **Add/Remove Templates**.
9. Navigate to %systemroot%\inf, select **Barracuda Message Archiver Search *version*.adm**, and click **Add**.

Configuration

Use the following steps to configure the Barracuda Message Archiver StandAlone Search Utility.

1. While still in the GPO Editor, navigate to **Computer Configuration > Administrative Templates**, and expand the Barracuda node that should now be visible.
2. Click **Message Archiver**, and click **Barracuda Message Archiver Search**.
3. Doubleclick the **Barracuda Message Archiver URI** policy, and enter the fully qualified URI that users are to use to access the Barracuda Message Archiver, for example, `http://archiver.mycompany.com:8000`. Note the following:
   - If users will be accessing the Barracuda Message Archiver from outside the local network, the URI must be externally accessible.
   - If users must use HTTPS when connecting, specify 'HTTPS' in the URI.
   - Remember to include the port number in the URI. If you have not changed the default port settings on your Barracuda Message Archiver, the HTTP port is 8000, and the HTTPS port (which need not be specified here) is 443.
4. Configure other settings as required. For an explanation of the available settings, click the **Explain** tab of the policy.

Deployment

Use the following steps to deploy the Microsoft installer (.**msi**) file.

1. Start the GPO Editor for the domain where you are installing the utility.
2. Either *edit* the default policy or create a new policy object, and link it to the desired container; for example, the particular OU containing the computers of users that will be using the utility.
3. Navigate to Computer **Configuration > Software Settings > Software Installation**, rightclick **Software Installation**, and click **New/Package**.
4. Enter the UNC path to the .msi located in the shared folder, and click **OK**.

Testing

Use the following steps to test Barracuda Message Archiver StandAlone Search Utility deployment.

Group Policy updates can take several minutes to post; run `gpupdate /force` to perform an immediate update.

1. Restart a computer that is joined to the domain.
2. Verify that the utility is installed when you log in, and the configured policies are applied.

Troubleshooting

Following is a list of troubleshooting tips.

- A common cause of failure is that the user and/or the user's computer does not have adequate access to the share location. Verify that all access and network privileges are configured appropriately.
- Additional error messages are available in the Event Log on the domain computer; if you do not find the desired information in the Event Log, consider enabling verbose logging and restarting the computer.
- For additional information on fixing Group Policy issues, see "Fixing Group Policy problems by using log files" on the Microsoft TechNet website.

Barracuda Message Archiver Stand-Alone Search Utility for Windows

This article refers to the Barracuda Message Archiver release 3.1 or higher.

You can download and install the Barracuda Message Archiver Stand-Alone Search Utility on your Windows-based system to allow archive searches without using either the Barracuda Message Archiver Outlook Add-In or logging in to the Barracuda Message Archiver web interface.

Install the Barracuda Message Archiver Search Utility

Use the following steps to install the Barracuda Message Archiver Stand-Alone Search Utility:

1. Log in to the Barracuda Message Archiver, and go to the **USERS > Client Downloads** page.
2. In the **Stand-Alone Search Utility** section, click **Download Now** to the right of the **Stand-Alone Search Utility** to download the **.msi** installer .
3. Locate and double-click the **.msi** file to open the **Setup Wizard**.
4. Follow the onscreen instructions to install the utility.

Set Up the Barracuda Message Archiver Search Utility

Use the following steps to set up the Barracuda Message Archiver Stand-Alone Search Utility:

1. Launch **Barracuda Message Archiver Search**.
2. In the setup dialog, enter the **URI of your Barracuda Message Archiver**, for example, `https://archiver.mycompany.com:8000`

   If you do not know the URI of your Barracuda Message Archiver, contact your administrator.
3. Enter your **Email Address** and **Password**, and then click **OK**.

You are now ready to search your message archives.

Barracuda Message Archiver Stand-Alone Search Utility for Mac OS X

This article refers to the Barracuda Message Archiver release 3.5 or higher.

You can download and install Barracuda Archive Search on your Mac OS X-based system to allow archive searches without logging in to the Barracuda Message Archiver web interface.

Install Barracuda Archive Search

Use the following steps to install Barracuda Archive Search:

1. Log in to the Barracuda Message Archiver, and go to the **USERS > Client Downloads** page.
2. In the **Stand-Alone Search Utility** section, click **Download Now** to the right of the **Mac Stand-Alone Search Utility** to download the **.dmg** file .
3. Locate and double-click the downloaded **.dmg** file to mount it.
4. Double-click the mounted volume on your desktop, and drag the app icon to the **Applications** icon in the Finder sidebar.

Set Up Barracuda Archive Search

Use the following steps to set up the Barracuda Archive Search:

1. Launch **Barracuda Archive Search**. The **Options** dialog box displays the first time you launch the utility.
2. In the **Options** dialog, enter the **Address** of your **Barracuda Message Archiver**, for example, `https://archiver.mycompany.com:8000`

If you don't know the address of your Barracuda Message Archiver, contact your administrator.

3. Enter your **Email Address** and **Password**, and then click **OK**.

You are now ready to search your message archives.

Hardware Compliance

This section contains appliance compliance information.

Notice for the USA

Compliance Information Statement (Declaration of Conformity Procedure) DoC FCC Part 15: This device complies with part 15 of the FCC Rules.

Operation is subject to the following conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received including interference that may cause undesired operation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user in encouraged to try one or more of the following measures:
    - Reorient or relocate the receiving antenna.
    - Increase the separation between the equipment and the receiver.
    - Plug the equipment into an outlet on a circuit different from that of the receiver.
    - Consult the dealer on an experienced radio/ television technician for help.

Notice for Canada

This apparatus complies with the Class B limits for radio interference as specified in the Canadian Department of Communication Radio Interference Regulations.

Notice for Europe (CE Mark)

This product is in conformity with the Council Directive 89/336/EEC, 92/31/EEC (EMC).

Power Requirements

AC input voltage 100-240 volts; frequency 50/60 Hz.

Limited Warranty and License

Limited Warranty

Barracuda Networks, Inc., or the Barracuda Networks, Inc. subsidiary or authorized Distributor selling the Barracuda Networks product, if sale is not directly by Barracuda Networks, Inc., (“Barracuda Networks”) warrants that commencing from the date of delivery to Customer (but in case of resale by a Barracuda Networks reseller, commencing not more than sixty (60) days after original shipment by Barracuda Networks, Inc.), and continuing for a period of one (1) year: (a) its products (excluding any software) will be free from material defects in materials and workmanship under normal use; and (b) the software provided in connection with its products, including any software contained or embedded in such products will substantially conform to Barracuda Networks published specifications in effect as of the date of manufacture. Except for the foregoing, the

software is provided as is. In no event does Barracuda Networks warrant that the software is error free or that Customer will be able to operate the software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Barracuda Networks does not warrant that the software or any equipment, system or network on which the software is used will be free of vulnerability to intrusion or attack. The limited warranty extends only to you the original buyer of the Barracuda Networks product and is non-transferable.

Exclusive Remedy

Your sole and exclusive remedy and the entire liability of Barracuda Networks under this limited warranty shall be, at Barracuda Networks or its service centers option and expense, the repair, replacement or refund of the purchase price of any products sold which do not comply with this warranty. Hardware replaced under the terms of this limited warranty may be refurbished or new equipment substituted at Barracuda Networks option. Barracuda Networks obligations hereunder are conditioned upon the return of affected articles in accordance with Barracuda Networks then-current Return Material Authorization (“RMA”) procedures. All parts will be new or refurbished, at Barracuda Networks discretion, and shall be furnished on an exchange basis. All parts removed for replacement will become the property of the Barracuda Networks. In connection with warranty services hereunder, Barracuda Networks may at its discretion modify the hardware of the product at no cost to you to improve its reliability or performance. The warranty period is not extended if Barracuda Networks repairs or replaces a warranted product or any parts. Barracuda Networks may change the availability of limited warranties, at its discretion, but any changes will not be retroactive. IN NO EVENT SHALL BARRACUDA NETWORKS LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION.

Exclusions and Restrictions

This limited warranty does not apply to Barracuda Networks products that are or have been (a) marked or identified as “sample” or “beta,” (b) loaned or provided to you at no cost, (c) sold “as is,” (d) repaired, altered or modified except by Barracuda Networks, (e) not installed, operated or maintained in accordance with instructions supplied by Barracuda Networks, or (f) subjected to abnormal physical or electrical stress, misuse, negligence or to an accident.

EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS MAKES NO OTHER WARRANTY, EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO BARRACUDA NETWORKS PRODUCTS, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, AVAILABILITY, RELIABILITY, USEFULNESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS PRODUCTS AND THE SOFTWARE IS PROVIDED “AS IS” AND BARRACUDA NETWORKS DOES NOT WARRANT THAT ITS PRODUCTS WILL MEET YOUR REQUIREMENTS OR BE UNINTERRUPTED, TIMELY, AVAILABLE, SECURE OR ERROR-FREE, OR THAT ANY ERRORS IN ITS PRODUCTS OR THE SOFTWARE WILL BE CORRECTED. FURTHERMORE, BARRACUDA NETWORKS DOES NOT WARRANT THAT BARRACUDA NETWORKS PRODUCTS, THE SOFTWARE OR ANY EQUIPMENT, SYSTEM OR NETWORK ON WHICH BARRACUDA NETWORKS PRODUCTS WILL BE USED WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK.

Software License

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT (“AGREEMENT”) CAREFULLY BEFORE USING THE BARRACUDA SOFTWARE. BY USING THE BARRACUDA SOFTWARE YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE DO NOT USE THE SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE YOU MAY RETURN THE SOFTWARE OR HARDWARE CONTAINING THE SOFTWARE FOR A FULL REFUND TO YOUR PLACE OF PURCHASE.

1. The software, documentation, whether on disk, in read only memory, or on any other media or in any other form (collectively “Barracuda Software”) is licensed, not sold, to you by Barracuda Networks, Inc. (“Barracuda”) for use only under the terms of this License and Barracuda reserves all rights not expressly granted to you. The rights granted are limited to Barracuda's intellectual property rights in the Barracuda Software and do not include any other patent or intellectual property rights. You own the media on which the Barracuda Software is recorded but Barracuda retains ownership of the Barracuda Software itself.

2. Permitted License Uses and Restrictions. This License allows you to use the Software only on the single Barracuda labeled hardware device on which the software was delivered. You may not make copies of the Software and you may not make the Software available over a network where it could be utilized by multiple devices or copied. You may not make a backup copy of the Software. You may not modify or create derivative works of the Software except as provided by the Open Source Licenses included below. The BARRACUDA SOFTWARE IS NOT INTENDED FOR USE IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, LIFE SUPPORT MACHINES, OR OTHER EQUIPEMENT IN WHICH FAILURE COULD LEAD TO DEATH, PERSONAL INJURY, OR ENVIRONMENTAL DAMAGE.

3. You may not transfer, rent, lease, lend, or sublicense the Barracuda Software.

4. This License is effective until terminated. This License is automatically terminated without notice if you fail to comply with any term of the License. Upon termination you must destroy or return all copies of the Barracuda Software.

5. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT THE USE OF THE BARRACUDA SOFTWARE IS AT YOUR OWN RISK AND THAT THE ENTIRE RISK AS TO SATISFACTION, QUALITY, PERFORMANCE, AND ACCURACY IS WITH YOU. THE BARRACUDA SOFTWARE IS PROVIDED “AS IS” WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND BARRACUDA HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE BARRACUDA SOFTWARE, EITHER EXPRESSED OR IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTIBILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR ANY APPLICATION, OF ACCURACY, AND OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS. BARRACUDA DOES NOT WARRANT THE CONTINUED OPERATION OF THE SOFTWARE, THAT THE PERFORMANCE WILL MEET YOUR EXPECTATIONS, THAT THE FUNCTIONS WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION WILL BE ERROR FREE OR CONTINUOUS, OR THAT DEFECTS WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION GIVEN BY BARRACUDA OR AUTHORIZED BARRACUDA REPRESENTATIVE SHALL CREATE A WARRANTY. SHOULD THE BARRACUDA SOFTWARE PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION.

6. License. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT YOU WILL PROVIDE AN UNLIMITED ZERO COST LICENSE TO BARRACUDA FOR ANY PATENTS OR OTHER INTELLECTUAL PROPERTY RIGHTS UTILIZED IN THE BARRACUDA SOFTWARE WHICH YOU EITHER OWN OR CONTROL.

7. Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL BARRACUDA BE LIABLE FOR PERSONAL INJURY OR ANY INCIDENTAL SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION, OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR ABILITY TO USE OR INABILITY TO USE THE BARRACUDA SOFTWARE HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY AND EVEN IF BARRACUDA HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. In no event shall Barracuda's total liability to you for all damages exceed the amount of one hundred dollars.

8. Export Control. You may not use or otherwise export or re-export Barracuda Software except as authorized by the United States law and the laws of the jurisdiction where the Barracuda Software was obtained.

Energize Update Software License

PLEASE READ THIS ENERGIZE UPDATE SOFTWARE LICENSE CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING BARRACUDA NETWORKS OR BARRACUDA NETWORKS-SUPPLIED ENERGIZE UPDATE SOFTWARE.

BY DOWNLOADING OR INSTALLING THE ENERGIZE UPDATE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS LICENSE. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE, THEN (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM BARRACUDA NETWORKS OR AN AUTHORIZED BARRACUDA NETWORKS RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL PURCHASER.

The following terms govern your use of the Energize Update Software except to the extent a particular program (a) is the subject of a separate written agreement with Barracuda Networks or (b) includes a separate “click-on” license agreement as part of the installation and/or download process. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the written agreement, (2) the click-on agreement, and (3) this Energize Update Software License.

License. Subject to the terms and conditions of and except as otherwise provided in this Agreement, Barracuda Networks, Inc., or a Barracuda Networks, Inc. subsidiary (collectively “Barracuda Networks”), grants to the end-user (“Customer”) a nonexclusive and nontransferable license to use the Barracuda Networks Energize Update program modules and data files for which Customer has paid the required license fees (the “Energize Update Software”). In addition, the foregoing license shall also be subject to the following limitations, as applicable:

Unless otherwise expressly provided in the documentation, Customer shall use the Energize Update Software solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Barracuda Networks equipment) for communication with Barracuda Networks equipment owned or leased by Customer; Customer's use of the Energize Update Software shall be limited to use on a single hardware chassis, on a single central processing unit, as applicable, or use on such greater number of chassis or central processing units as Customer may have paid Barracuda Networks the required license fee; and Customer's use of the Energize Update Software shall also be limited, as applicable and set forth in Customer's purchase order or in Barracuda Networks' product catalog, user documentation, or web site, to a maximum number of (a) seats (i.e. users with access to the installed Energize Update Software), (b) concurrent users, sessions, ports, and/or issued and outstanding IP addresses, and/or (c) central processing unit cycles or instructions per second. Customer's use of the Energize Update Software shall also be limited by any other restrictions set forth in Customer's purchase order or in Barracuda Networks' product catalog, user documentation or web site for the Energize Update Software.

General Limitations. Except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

i. transfer, assign or sublicense its license rights to any other person, or use the Energize Update Software on unauthorized or secondhand Barracuda Networks equipment, and any such attempted transfer, assignment or sublicense shall be void;
ii. make error corrections to or otherwise modify or adapt the Energize Update Software or create derivative works based upon the Energize Update Software, or to permit third parties to do the same; or
iii. decompile, decrypt, reverse engineer, disassemble or otherwise reduce the Energize Update Software to human-readable form to gain access to trade secrets or confidential information in the Energize Update Software.

Upgrades and Additional Copies. For purposes of this Agreement, “Energize Update Software” shall include (and the terms and conditions of this Agreement shall apply to) any Energize Update upgrades, updates, bug fixes or modified versions (collectively, “Upgrades”) or backup copies of the Energize Update Software licensed or provided to Customer by Barracuda Networks or an authorized distributor/reseller for which Customer has paid the applicable license fees. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY SUCH ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL ENERGIZE UPDATE SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE; (2) USE OF UPGRADES IS LIMITED TO BARRACUDA NETWORKS EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE ENERGIZE UPDATE SOFTWARE WHICH IS BEING UPGRADED; AND (3) USE OF ADDITIONAL COPIES IS LIMITED TO BACKUP PURPOSES ONLY.

Energize Update Changes. Barracuda Networks reserves the right at any time not to release or to discontinue release of any Energize Update Software and to alter prices, features, specifications, capabilities, functions, licensing terms, release dates, general availability or other characteristics of any future releases of the Energize Update Software.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Energize Update Software in the same form and manner that such copyright and other proprietary notices are included on the Energize Update Software. Except as expressly authorized in this Agreement, Customer shall not make any copies or duplicates of any Energize Update Software without the prior written permission of Barracuda Networks. Customer may make such backup copies of the Energize Update Software as may be necessary for Customer's lawful use, provided Customer affixes to such copies all copyright, confidentiality, and proprietary notices that appear on the original.

Protection of Information. Customer agrees that aspects of the Energize Update Software and associated documentation, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Barracuda Networks. Customer shall not disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of Barracuda Networks. Customer shall implement reasonable security measures to protect and maintain the confidentiality of such trade secrets and copyrighted material. Title to Energize Update Software and documentation shall remain solely with Barracuda Networks.

Indemnity. Customer agrees to indemnify, hold harmless and defend Barracuda Networks and its affiliates, subsidiaries, officers, directors, employees and agents at Customers expense, against any and all third-party claims, actions, proceedings, and suits and all related liabilities, damages, settlements, penalties, fines, costs and expenses (including, without limitation, reasonable attorneys fees and other dispute resolution expenses) incurred by Barracuda Networks arising out of or relating to Customers (a) violation or breach of any term of this Agreement or any policy or guidelines referenced herein, or (b) use or misuse of the Barracuda Networks Energize Update Software.

Term and Termination. This License is effective upon date of delivery to Customer of the initial Energize Update Software (but in case of resale by a Barracuda Networks distributor or reseller, commencing not more than sixty (60) days after original Energize Update Software purchase from Barracuda Networks) and continues for the period for which Customer has paid the required license fees. Customer may terminate this License at any time by notifying Barracuda Networks and ceasing all use of the Energize Update Software. By terminating this License, Customer forfeits any refund of license fees paid and is responsible for paying any and all outstanding invoices. Customer's rights under this License will terminate immediately without notice from Barracuda Networks if Customer fails to comply with any provision of this License. Upon termination, Customer must cease use of all copies of Energize Update Software in its possession or control.

Export. Software, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Energize Update Software.

Restricted Rights. Barracuda Networks' commercial software and commercial computer software documentation is provided to United States Government agencies in accordance with the terms of this Agreement, and per subparagraph “(c)” of the “Commercial Computer Software - Restricted Rights” clause at FAR 52.227-19 (June 1987). For DOD agencies, the restrictions set forth in the “Technical Data-Commercial Items” clause at DFARS 252.227-7015 (Nov 1995) shall also apply.

No Warranty. The Energize Update Software is provided AS IS. Customer's sole and exclusive remedy and the entire liability of Barracuda Networks under this Energize Update Software License Agreement will be, at Barracuda Networks option, repair, replacement, or refund of the Energize Update Software.

Renewal. At the end of the Energize Update Service Period, Customer may have the option to renew the Energize Update Service at the current

list price, provided such Energize Update Service is available. All initial subscriptions commence at the time of sale of the unit and all renewals commence at the expiration of the previous valid subscription.

In no event does Barracuda Networks warrant that the Energize Update Software is error free or that Customer will be able to operate the Energize Update Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Barracuda Networks does not warrant that the Energize Update Software or any equipment, system or network on which the Energize Update Software is used will be free of vulnerability to intrusion or attack.

DISCLAIMER OF WARRANTY. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

General Terms Applicable to the Energize Update Software License Disclaimer of Liabilities. IN NO EVENT WILL BARRACUDA NETWORKS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE ENERGIZE UPDATE SOFTWARE EVEN IF BARRACUDA NETWORKS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Barracuda Networks' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

This Energize Update Software License shall be governed by and construed in accordance with the laws of the State of California, without reference to principles of conflict of laws, provided that for Customers located in a member state of the European Union, Norway or Switzerland, English law shall apply. The United Nations Convention on the International Sale of Goods shall not apply. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Energize Update Software License shall remain in full force and effect. Except as expressly provided herein, the Energize Update Software License constitutes the entire agreement between the parties with respect to the license of the Energize Update Software and supersedes any conflicting or additional terms contained in the purchase order.

Open Source Licensing

Barracuda products may include programs that are covered by the GNU General Public License (GPL) or other “open source” license agreements. The GNU license is re-printed below for you reference. These programs are copyrighted by their authors or other parties, and the authors and copyright holders disclaim any warranty for such programs. Other programs are copyright by Barracuda Networks.

GNU GENERAL PUBLIC LICENSE, (GPL) Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public

License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If

the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
>
> b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
>
> c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

> a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT

NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Barracuda Products may contain programs that are copyright (c)1995-2005 International Business Machines Corporation and others. All rights reserved. These programs are covered by the following License:

"Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation."

Barracuda Products may include programs that are covered by the BSD License: "Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.''

Barracuda Products may include the libspf library which is Copyright (c) 2004 James Couzens & Sean Comeau All rights reserved. It is covered by the following agreement: Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS MAKING USE OF THIS LICENSE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Products may contain programs that are Copyright (c) 1998-2003 Carnegie Mellon University. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact Office of Technology Transfer Carnegie Mellon University 5000 Forbes Avenue Pittsburgh, PA 15213-3890 (412) 268-4387, fax: (412) 268-7395 tech-transfer@andrew.cmu.edu .Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)." CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Barracuda products may include programs that are covered by the Apache License or other Open Source license agreements. The Apache license is re-printed below for you reference. These programs are copyrighted by their authors or other parties, and the authors and copyright holders disclaim any warranty for such programs. Other programs are copyright by Barracuda Networks.

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License.

You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without

limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Source Code Availability
Per the GPL and other “open source” license agreements the complete machine readable source code for programs covered by the GPL or other “open source” license agreements is available from Barracuda Networks at no charge. If you would like a copy of the source code or the changes to a particular program we will gladly provide them, on a CD, for a fee of $100.00. This fee is to pay for the time for a Barracuda Networks engineer to assemble the changes and source code, create the media, package the media, and mail the media. Please send a check payable in USA funds and include the program name. We mail the packaged source code for any program covered under the GPL or other "open source" license.

Document Downloads

Quick Start Guides (PDF)

- Barracuda Message Archiver Quick Start Guide - US
- Barracuda Message Archiver Quick Start Guide - German
- Barracuda Message Archiver Quick Start Guide - Chinese
- Barracuda Message Archiver Quick Start Guide - Japanese

Deployment Templates, Tools, and Utilities (PDF)

To download tools and utilities, go to the **USERS > Client Downloads** page in the Barracuda Message Archiver web interface.

- Microsoft Exchange Server 2003 Deployment Template
- Microsoft Exchange Server 2007-2010 Deployment Template
- Configuring an SMTP Journal Account for Microsoft Exchange 2003
- Envelope Journaling for Microsoft Exchange 2007/2010
- Barracuda Message Archiver Standalone Search Utility